Facultade de Informática
UNIVERSIDADE DA CORUÑA

TRABALLO FIN DE GRAO
GRAO EN ENXEÑARÍA INFORMÁTICA
MENCIÓN EN TECNOLOXÍAS DA INFORMACIÓN

PESCI: Plataforma de Entrega de Servicios Cloud para Investigación

Estudante: Amaro Castro Faci
Dirección: Antonio Daniel López Rivas
Jose Carlos Dafonte Váquez

A Coruña, outubro de 2020.

Resumen

El Cloud Computing es un modelo que permite acceder a un conjunto de recursos, como por ejemplo redes, almacenamiento y cómputo, los cuales pueden ser aprovisionados bajo demanda de forma automatizada y dinámica, reduciendo el coste del servicio para el usuario y el esfuerzo en cuanto a la administración de los recursos. El Centro de Investigación en Tecnoloxías da Información e as Comunicacións (CITIC) de la Universidade da Coruña cuenta con una infraestructura ideada para ofrecer un servicio de Cloud Computing a la comunidad universitaria. Este servicio consiste en que los usuarios aprovisionan un conjunto de recursos, del tamaño que requieran para la realización de tareas que no serían posibles en dispositivos convencionales. Actualmente ese servicio está activo pero de forma limitada y no abierta a todos los usuarios del CITIC, debido a que no existe una plataforma que permita gestionar los perfiles de usuario ni su autenticación, ni un portal de acceso para aprovisionar recursos y gestionarlos de forma automatizada. En la actualidad, las tareas de aprovisionamiento y gestión de usuarios se realizan bajo petición previa al administrador del sistema, que las ejecuta de forma manual, lo cual produce gran coste en tiempo y recursos, y aumenta los riesgos del servicio.

Este proyecto consiste en desplegar un servicio Cloud en el CITIC, usando como base la infraestructura y herramientas ya existentes. El servicio debe proveer un sistema de autenticación para que cada usuario pueda acceder con sus credenciales de la UDC a una plataforma, la cual le permita aprovisionar y gestionar recursos de forma automatizada y dinámica. Además, también debe automatizar la gestión de todos los componentes de la infraestructura, incluyendo perfiles de usuarios, la cantidad de recursos disponibles para los usuarios y el despliegue de aplicaciones por parte de los usuarios, con el fin de liberar a los administradores de las tareas más redundantes y repetitivas. De esta forma, se persigue obtener el máximo rendimiento de la infraestructura disponible en el CITIC.

Palabras clave:

- Cloud Computing
- CITIC
- Virtualización
- SDDC
- Aprovisionamiento

Índice general

1 Introducción **1**

1.1 Motivación 2

1.2 Objetivos 3

1.3 Organización 3

2 Estado de los recursos **5**

2.1 Infraestructura 5

2.1.1 Cómputo 5

2.1.2 Almacenamiento 5

2.1.3 Red 6

2.2 Software 6

2.3 Estado de la tecnología 9

2.3.1 VMware Cloud Foundation 9

2.3.2 Componentes de VMware Cloud Foundation 11

3 Planificación **15**

3.1 Tareas 15

3.2 Costes 19

4 Metodología **21**

4.1 Conceptos 21

4.1.1 Workload Domain 21

4.1.2 Arquitectura 22

4.1.3 Clusters, zonas y distribución de un SDDC 24

4.2 Requisitos 26

4.2.1 Cómputo 26

4.2.2 Almacenamiento 26

4.2.3 Red 27

4.3 Prueba de concepto 28
4.3.1 Preparación 28
4.3.2 Diseño y configuración del Management Domain 30
4.3.3 Operaciones de la Arquitectura 38

A Material adicional **49**

Notas **53**

Lista de acrónimos **55**

Glosario **57**

Bibliografía **59**

Índice de figuras

2.1 Componentes de VMware vSphere[1] 7
2.2 Componentes físicos y software que forman la infraestructura actual. 8
2.3 Estructura de VMare Cloud Foundation. 10
2.4 Elementos de un SDDC gestionado con VMware Cloud Foundation. 11
2.5 Partes de un SDDC y componentes de VCF que las implementan. 11
2.6 Configuración *All-Flash* y configuración *Hybrid* en vSAN 12
2.7 Componentes de VMware NSX-T y capas en las que se dividen 13

3.1 Diagrama de Grantt sobre la planificación del proyecto. 18
3.2 Estadísticas sobre la planificación del proyecto. 19

4.1 Esquema del modelo de arquitectura estándar. 23
4.2 Esquema del modelo de arquitectura consolidado. 24
4.3 Ejemplo de un SDDC con dos Regions y una AZ en cada uno. 25
4.4 Herramienta VMware Lab Constructor v4.0.1b 29
4.5 Elementos desplegados en el host físico. 30
4.6 Dominio y cluster vSphere del Management Domain. 31
4.7 Ejemplo de como se almacena un archivo con VMware vSAN y FTT igual a uno 32
4.8 Contenido de vSphere Distributed Switch *sddc-vds01*. 34
4.9 Segments a los que se conecta cada nodo de VMware NSX-T y como acceden a la red física. 36
4.10 Topología virtual de VMware NSX-T 37
4.11 Componentes con los que se comunica vRSLCM. 39
4.12 Apartado donde se muestra la configuración de la instancia de WSA en vRSLCM. 40
4.13 Usuarios dentro de Active Directory 41
4.14 Sincronización de usuarios desde Workspace One Access. 41
4.15 Usuarios sincronizados en Workspace One Access. 41
4.16 Política de autenticación por defecto. 42

4.17 Plataforma de autenticación de Workspace One Access 43
4.18 Uso y componentes de VMware vRealize Automation. 44
4.19 Nuevo Segment *vra-deployments* en el router virtual Tier-1. 45
4.20 Configuración del servicio cloud-init en Ubuntu Server 20. 45
4.21 Creación de una plantilla a partir de la VM de Ubuntu Server 20. 46

Capítulo 1

Introducción

Según *National Institute of Standards and Technology* (NIST), «Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources»[2]. Las principales características de este modelo son:

- *Autoservicio bajo demanda*: El usuario puede aprovisionar recursos según sus necesidades y de forma automática sin requerir ninguna interacción humana con el proveedor del servicio.
- *Acceso por red*: El servicio está disponible para los usuarios a través de red de forma remota.
- *Almacén de recursos*: Los recursos son accesibles por múltiples usuarios simultáneamente, y todos ellos acceden a la misma instancia del software que gestiona el servicio, siendo este un servicio *multi-tenant*.
- *Elasticidad*: Los recursos se pueden aprovisionar o liberar de forma elástica, es decir, se pueden escalar de forma rápida según las necesidades del usuario.
- *Servicio medido*: El servicio Cloud es capaz de obtener y abstraer información acerca del consumo de recursos para monitorizarlos, controlarlos e informar al usuario y al proveedor.

El Centro de Investigación en Tecnoloxías da Información e as Comunicacións (CITIC) de la Universidade da Coruña, cuenta con una infraestructura construida para ofrecer un servicio Cloud al personal que trabaja en sus instalaciones, y así darles acceso a hardware que no está disponible en dispositivos convencionales. Actualmente, esta infraestructura tiene instalado un software de virtualización la empresa VMware, pero que no cuenta con los elementos suficientes para ser accedido por todos los usuarios. Este servicio de virtualización permite aprovisionar recursos de un conjunto de servidores, en forma de máquinas virtuales con unas

especificaciones establecidas por el usuario, para realizar tareas que requieren gran capacidad de cómputo, de almacenamiento o de red.

El sistema cuenta con una plataforma de autenticación, pero los usuarios a los que está destinado el servicio no tienen acceso. Esto se debe a que no existe una herramienta que permita gestionar perfiles de usuario ya existentes, sino que, el único modo de habilitar el acceso consiste en que el administrador cree una perfil de forma manual dentro del servicio para cada usuario. También carece de una plataforma donde cada usuario solo tenga acceso a sus recursos, en la vista actual tienen visibilidad y acceso a los recursos de otros usuarios dependiendo de los permisos que se hayan asignado al perfil. Además, en el sistema actual, el proceso de aprovisionamiento de recursos mediante la creación de máquinas virtuales es complejo, por tener una interfaz poco intuitiva y difícil de manejar para un usuario que no es administrador del sistema, a parte de que el proceso debe realizarse manualmente. Esto implica que la monitorización, control y medición de los recursos que aprovisiona cada usuario sean también complejas. La falta de automatización y simplicidad en el sistema provoca que el administrador tenga que gestionar todo el entorno de forma manual, tanto los perfiles de usuarios como los recursos y su configuración, lo cual genera un gran coste y aumenta los riesgos de la infraestructura.

Como se puede observar, el servicio no cumple con las características que definen un servicio de Cloud Computing, especialmente en lo que se refiere al aprovisionamiento bajo demanda, a la elasticidad y a la monitorización y control de los recursos. Por ello, en este proyecto se desplegará un conjunto de servicios, que juntos permitan habilitar un servicio al que los usuarios puedan acceder autenticándose con sus credenciales de la UDC, aprovisionar recursos de red, almacenamiento y cómputo, y que permita monitorizar los recursos que cada usuario posee. Además, para facilitar las tareas de administración, el servicio debe automatizar las operaciones de aprovisionamiento y permitir al administrador limitar la cantidad de recursos que un usuario puede aprovisionar para evitar que estos sean infrautilizados. Con estas mejoras se busca construir un servicio que sea útil, dinámico, sencillo de administrar, que optimice el uso de los recursos y que aumente su eficiencia, gracias a la automatización de tareas y al aprovechamiento de elementos que ya se encuentran disponibles.

1.1 Motivación

La motivación para realizar este proyecto es crear un servicio Cloud en el CITIC para proporcionar recursos a aquellos usuarios que necesiten equipos de grandes prestaciones, y que estos los puedan conseguir de una forma sencilla y ágil, a la vez que se mejora la gestión interna del servicio para así reducir sus costes e incidencias a largo plazo. En definitiva, hacer que la infraestructura sea eficiente, útil y capaz de dar servicio a todos sus usuarios.

1.2 Objetivos

El objetivo general de este proyecto es crear un servicio piloto, desplegando sobre un entorno de pruebas, y presentar las funcionalidades y características de una plataforma que permita sacar el máximo rendimiento de la infraestructura del CITIC, y de los recursos administrativos que se encuentran disponibles, tanto en el CITIC como en la UDC. Este servicio debe ser útil, ágil y accesible. Los objetivos concretos se pueden resumir en los siguientes puntos:

- Centralizar y mejorar la gestión de usuarios integrando el sistema de autenticación de la UDC y así facilitar el acceso.
- Desplegar un portal de acceso para los usuarios que simplifique la gestión y aprovisionamiento de sus recursos.
- Limitar y controlar la cantidad de recursos que un usuario puede aprovisionar y así evitar tener recursos ociosos.
- Automatizar las tareas de administración y configuración de la infraestructura.
- Documentar las soluciones desplegadas en el sistema para facilitar la transmisión de conocimiento a largo plazo.

1.3 Organización

La documentación de este proyecto se divide en cinco capítulos. El primero es 2.Estado de los recursos y en él se describe el hardware y el software que forman la infraestructura situada en el CITIC, la situación actual de la tecnología que se quiere implementar, las alternativas encontradas en el mercado y la descripción y componentes de la solución elegida. Posteriormente, en capítulo 3.Planificación se describen las tareas y los costes de la realización del proyecto en base a la solución elegida en el capítulo anterior. Una vez expuestas las tareas del proyecto, en el capítulo 4.Metodología se describen conceptos referidos a la infraestructura y arquitectura propios de la solución que se va a implementar, los requisitos físicos y servicios que la infraestructura debe proveer antes de realizar la implementación. Finalmente, dentro del mismo capítulo en el apartado 4.3. Prueba de concepto, se exponen la instalación y funcionalidades de los componentes de la solución propuesta, dentro de un entorno de pruebas.

Capítulo 2

Estado de los recursos

Con el fin de contextualizar los recursos utilizados para el desarrollo del proyecto, en este capítulo se expone la situación actual de la infraestructura situada en el CITIC. Esto incluye el software que está en funcionamiento, los recursos físicos de los que se compone, y el estado actual de las herramientas que rodean a dichos recursos.

2.1 Infraestructura

La infraestructura física donde se encuentra el servicio de virtualización, se encuentra en el edificio del CITIC de la UDC, dentro de un rack alojado en su Centro de Proceso de Datos (CPD)[3].

2.1.1 Cómputo

Está formada por 5 hosts Lenovo NeXtScale nx360 M5, cada uno con dos procesadores Intel Xeon E5-2650, 128 GB de memoria RAM y una tarjeta gráfica Tesla M60, y 3 hosts Dell EMC PowerEdge R740 cada uno con dos procesadores Xeon Gold 6146, 384 GB de memoria RAM y una tarjeta gráfica Tesla P40. Todos ellos aportan flexibilidad en cuanto a que permiten escalar la infraestructura y ofrecen gran rendimiento de cómputo.

2.1.2 Almacenamiento

El sistema de almacenamiento está colocado físicamente en la misma ubicación que los hosts pero en su abstracción lógica este es independiente y está separado de cada host. Está conformado por 13 discos duros SSD de 3.84 TB de capacidad, obteniendo así una cantidad total de casi 50 TB, pero su capacidad útil es de 34 TB ya que se utiliza la configuración de almacenamiento RAID 5 para aporta mayor integridad de los datos, mayor tolerancia a fallos y mayor ancho de banda. Los discos duros están colocados en una misma cabina formando un *pool* de almacenamiento que se divide en cinco LUNs (Logical Storage Unit) de 2 TB cada una,

representadas en el software de virtualización como cinco datastores, y que emplean el sistema de archivos VMFS propio de la compañía VMware, el cual optimiza el almacenamiento de máquinas virtuales. La configuración y gestión de este sistema se tiene que realizar al nivel de la capa física, por lo tanto si se quiere realizar un despliegue en el sistema de virtualización que requiera una configuración de almacenamiento diferente a la existente, como por ejemplo un sistema RAID con diferentes características, sería necesario modificar la configuración del sistema físico, siendo muy costoso en tiempo y riesgos. Por lo tanto, este sistema de almacenamiento no permite ajustar de forma precisa, rápida y bajo demanda la configuración de almacenamiento que un usuario requiera para sus aplicaciones.

2.1.3 Red

El sistema de almacenamiento forma una Storage Area Network (SAN), para ello se utilizan conexiones de tipo 10 Gbit entre los hosts y las cabinas donde se encuentran los discos duros. Para soportar este tipo de conexiones, cada cabina incorpora dos controladores con conectores de tipo SFP+. Además, las cabinas de almacenamiento incorporan otros dos puertos de 1 Gbit para llevar a cabo la administración de los discos. En esta estructura se utilizan los protocolos de red Ethernet y iSCSI. Para mantener la disponibilidad del acceso al sistema de almacenamiento y aumentar la disponibilidad de de las conexiones entre hosts, cada host de ellos se conecta a dos switches *trunk* para establecer rutas redundantes. Igual que con el sistema de almacenamiento, si se requieren realizar modificaciones sobre la red para adaptarse a los requisitos de un determinado despliegue, habría que hacerlas directamente sobre la red física. Esto puede generar problemas en la conectividad del entorno a parte de generar gran coste de tiempo.

2.2 Software

Actualmente, el software desplegado sobre la infraestructura está formado por los productos de la compañía VMware, uno de los principales proveedores de software de virtualización. Todos los componentes instalados se engloban dentro del producto **VMware vSphere**, en su versión 6.7, el cual contiene lo necesario para virtualizar la infraestructura junto con las herramientas para entregar el servicio y gestionar la infraestructura virtual. A continuación se describen los principales componentes que tiene VMware vSphere y que están instalados en la infraestructura.

En cada host está instalado el hipervisor ESXi de tipo baremetal, este se encarga de habilitar la virtualización de los recursos. Sobre los hosts se ecuentra una VM que alberga el servicio VMware vCenter Server, el cual actúa como centro de administración de todas las máquinas virtuales (VMs) y hosts que forman la infraestructura. Además, esta instancia de VMware

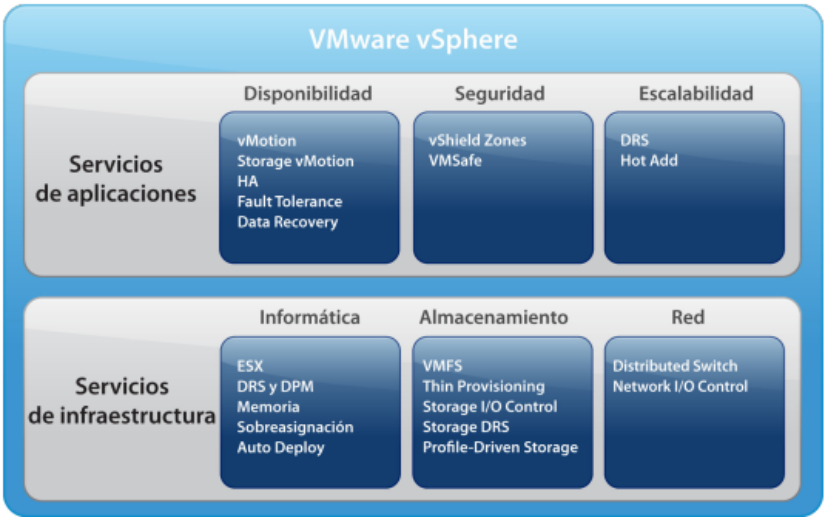


Figura 2.1: Componentes de VMware vSphere[1]

vCenter Server contiene una instancia embebida de Platform Services Controller (PSC), punto que centraliza la autenticación en las APIs de VMware vCenter Server, actúa como servidor de licencias y contiene servicio de autenticación de usuarios llamado vCenter Single Sign-On, este último se utiliza para gestionar la autenticación de los usuarios registrados en VMware vCenter Server. El acceso e interfaz de VMware vCenter Server la proporciona el componente vSphere Web Client, una página web donde el usuario puede autenticarse y gestionar las VMs y hosts que forman el entorno y el resto de servicios de VMware vSphere. Además, incorpora vSphere Update Manager desde el cual se gestionan las actualizaciones de los componentes de VMware vSphere. Para administrar las conexiones de las VMs desplegadas en el entorno, se utiliza el componente vSphere Distributed Switch (vDS), un switch virtual donde se establecen puertos para que las VMs tengan acceso a la red y a través de los cuales se configuran las propiedades del tráfico. Finalmente, se utilizan varios servicios de gran importancia para mantener la disponibilidad de las VMs desplegadas en la infraestructura:

- vMotion: encarga de migrar VMs de un host a otro de forma transparente y sin detener su ejecución ni el servicio.
- vSphere High Availability (HA): encargado de recuperar el servicio de una VM que ha sufrido un fallo. Para ello, la VM es reiniciada en otro host del entorno.
- vSphere Distributed Resource Scheduler (DRS): encargado de balancear la carga de trabajo entre los hosts disponibles en el entorno, migrando las VMs cuando sea necesario para maximizar el rendimiento de la infraestructura.

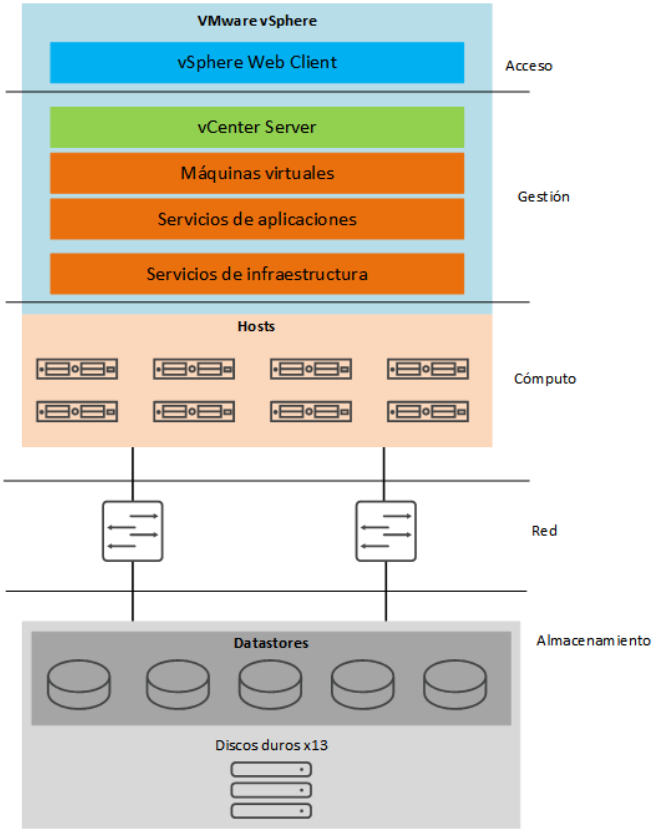


Figura 2.2: Componentes físicos y software que forman la infraestructura actual.

2.3 Estado de la tecnología

Con el desarrollo de las tecnologías web y la comercialización por parte de grandes empresas de su infraestructura, los servicios *Infrastructure as a Service* (IaaS) han ganado una popularidad considerable, con ello también se han desarrollado herramientas software dedicadas a la gestión de infraestructura para la implementación de sistemas Cloud Computing. Algunas de estas son VMware Cloud Foundation (creado en 2011), OpenStack (creado en 2010) o Apache CloudStack (creado en 2012). Estos productos proveen software que permite construir una infraestructura virtualizada sobre un conjunto de recursos físicos, con el objetivo de separar la administración de la capa física de la capa virtual, y simplificar y automatizar la gestión y escalabilidad de los recursos. Proponen un modelo que persigue reducir costes de gestión de la infraestructura y aumentar la disponibilidad del servicio, es decir, aumentar la eficiencia de la infraestructura física.

Como ya se ha visto, en el mercado existen varias alternativas que se pueden utilizar para cumplir los objetivos del proyecto. Finalmente, se ha escogido el producto **VMware Cloud Foundation** (VCF) ya que se integra perfectamente con los componentes de VMware ya instalados en la infraestructura y, por lo tanto, su mantenimiento sencillo. Desplegar un producto de una compañía diferente e integrarlo con los elementos desplegados en el CITIC, podría producir problemas de compatibilidad entre versiones a largo plazo, a pesar de que este se pueda integrar con el software VMware vSphere. Utilizando los productos de un mismo proveedor se asegura el soporte del software instalado y la obtención del máximo rendimiento de cada componente. Para poder usar este software es necesaria la adquisición de licencias. Estas se organizan por componente y por número de hosts sobre los que se va a instalar el producto. Aunque tienen un coste elevado, este producto aporta grandes beneficios.

2.3.1 VMware Cloud Foundation

Esta solución de VMware virtualiza todas las capas de la infraestructura combinando cuatro de sus productos. Utiliza **VMware vSphere** para virtualizar y gestionar el cómputo, **VMware vSAN** para virtualizar y gestionar el almacenamiento, **VMware NSX-T** para la virtualización y gestión de la red, y **VMware vRealize Suite** para gestionar las operaciones de la infraestructura virtual como el aprovisionamiento de recursos. Todos estos servicios juntos convierten el CPD en un Software Defined Datacenter (SDDC), un entorno donde existe una infraestructura física que se abstrae en una capa virtual para separar la gestión de ambas y poder modificar la infraestructura virtual según las necesidades de los usuarios sin necesidad de modificar la configuración de la infraestructura física, y que permite a los usuarios aprovisionar recursos, construyendo así un servicio de Cloud Computing. Con esta estructura se obtienen las siguientes características:

- Servicios software con integración nativa: ofrece un conjunto de servicios software para el almacenamiento, red, seguridad y gestión del servicio Cloud. Estos servicios se integran de forma nativa con la infraestructura minimizando las tareas de configuración y administración.
- Escalabilidad y elasticidad de los recursos: la capacidad de la infraestructura se puede modificar de forma sencilla gracias a la automatización del ciclo de vida de todos los elementos y al desacople entre las dos capas (la física y la virtual).
- Supervisión de los recursos: monitoriza los recursos con reconocimiento de aplicaciones y solución de problemas, permitiendo conocer todos los eventos que tienen lugar en la infraestructura. También permite establecer políticas de seguridad en cuanto al acceso a los recursos y la red.
- Aprovisionamiento automatizado: permite la obtención de recursos de forma automática incluyendo servicios de red, almacenamiento y cómputo. Los componentes de la infraestructura virtualizada se encargan de la reserva de los recursos y de todas las operaciones necesarias para llevarla acabo.
- Ciclo de vida automatizado: automatiza las operaciones de gestión previas, iniciales y posteriores de la plataforma para simplificar y coordinar su gestión. En estas tareas incluye el despliegue de la plataforma y su implementación, la escalabilidad de los recursos físicos y la instalación de actualizaciones para cada componente software.

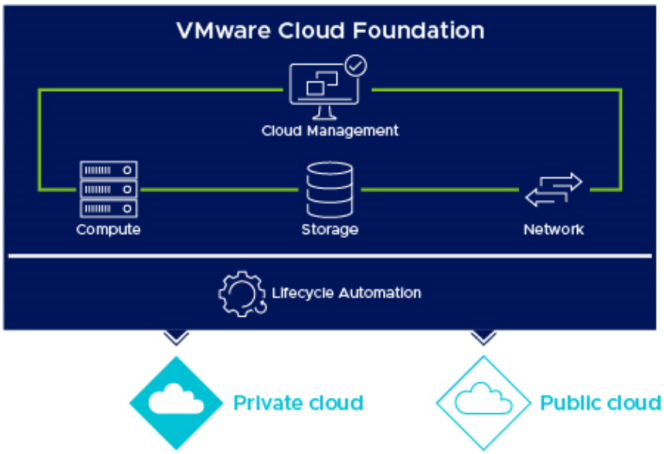


Figura 2.3: Estructura de VMare Cloud Foundation.

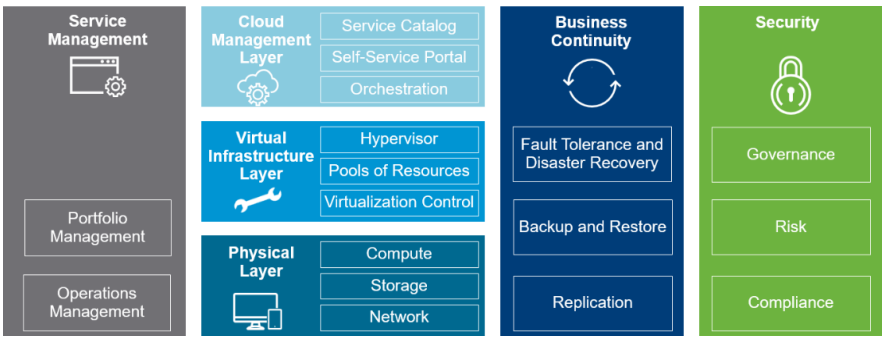


Figura 2.4: Elementos de un SDDC gestionado con VMware Cloud Foundation.

2.3.2 Componentes de VMware Cloud Foundation

Ya se ha visto que VCF está formado por cuatro productos principales. En este apartado se describirán las características de esos cuatro componentes más el servicio que los coordina[1]. Se utilizará la versión 4.0 de VMware Cloud Foundation lo cual implica que se implementarán las versiones[4] 4.0 de SDDC Manager, 7.0.0 de VMware vSphere, 7.0.0 de VMware vSAN, 3.0 de VMware NSX-T y 8.1 de VMware vRealize Suite.

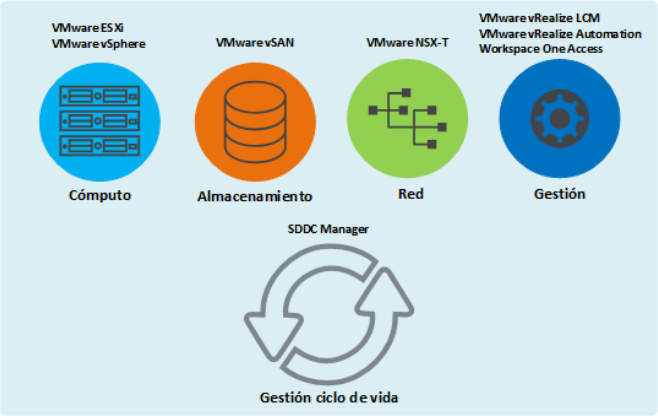


Figura 2.5: Partes de un SDDC y componentes de VCF que las implementan.

SDDC Manager

SDDC Manager se encarga de gestionar el ciclo de vida de todos los componentes de VCF, esto incluye el despliegue de cada uno, su configuración y la obtención e instalación de actualizaciones. Centraliza la gestión de las licencias y certificados de cada componente y administra el aprovisionamiento de nuevos recursos físicos para el SDDC y los ya existentes.

[1]Las características del componente VMware vSphere son las mismas que las descritas en el punto 2.2

VMware vSAN

VMware vSAN virtualiza el almacenamiento del SDDC. Permite gestionar de forma centralizada, desde la interfaz de vSphere Web Client, el sistema de almacenamiento sin necesidad de tener que modificar la configuración física. El sistema de almacenamiento se abstrae para formar único datastore sobre el que se establecen políticas de uso y disponibilidad. El acceso por parte de cada host al datastore se realiza con el protocolo IP, a través de una subred dedicada al servicio. Con VMware vSAN, el datastore está formado por discos de almacenamiento que se organizan en grupos que se asignan a un host. Los grupos pueden tener configuración *Hybrid*, que combina discos HDD y SDD, o configuración *All-Flash* que solo utiliza SSD y por lo tanto tiene mayor rendimiento. Dentro de cada grupo existe un disco de caché y al menos un disco de capacidad donde se almacenan los datos persistentes[5].

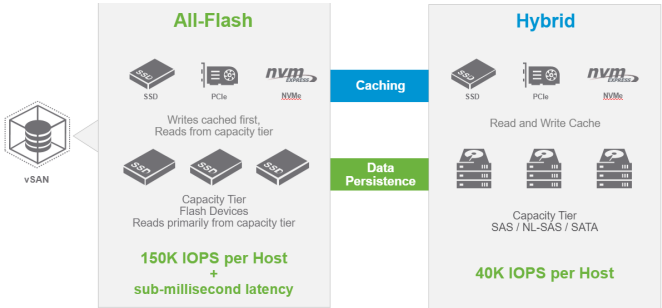


Figura 2.6: Configuración *All-Flash* y configuración *Hybrid* en vSAN

VMware NSX-T

VMware NSX-T virtualiza la red del SDDC. Abstrae los componentes físicos de la red para generar una red virtual desacoplada de la infraestructura física, esta se configura sin modificar la red física y para ello aporta servicios de red virtualizados y la posibilidad de crear y extender subredes sobre la infraestructura. Internamente tiene tres componentes, NSX-T Manager, NSX-T Controller y NSX-T Edge. El primero, es el punto de acceso a la configuración de VMware NSX-T y el que almacena y transmite la configuración establecida, el segundo controla las redes y se encarga de informar sobre el estado y la configuración de las redes virtuales. El último componente, NSX-T Edge, proporciona servicios de red y enrutamiento a las redes virtuales. Los hosts que están integrados en VMware NSX-T se encargan de controlar el tráfico y monitorizar las conexiones que mantiene VMware NSX-T.

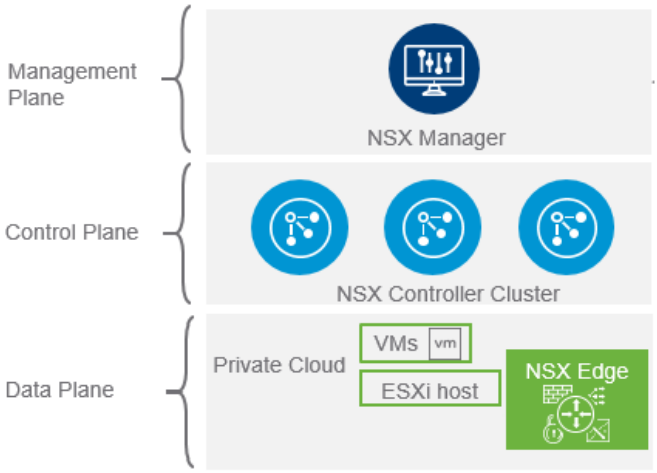


Figura 2.7: Componentes de VMware NSX-T y capas en las que se dividen

VMware vRealize Suite

VMware vRealize Suite agrupa un conjunto de productos que si bien no son obligatorios para desplegar VCF, aportan funcionalidades extra que completan la formación del SDDC y del servicio Cloud. Los productos que se utilizarán en este proyecto son **vRealize Suite Lifecycle Manager** dedicado a gestionar el despliegue, actualizaciones, certificados y licencias de los productos que forman VMware vRealize, **Workspace One Access** dedicado a gestionar los usuarios y ser el punto de acceso centralizado de las aplicaciones de VMware vRealize Suite y, finalmente, **vRealize Automation** el cual permite a los usuarios del SDDC diseñar y aprovisionar un conjunto de recursos de la infraestructura según sus necesidades y de forma automatizada mientras el administrador puede limitar la cantidad de recursos que se consumen.

Capítulo 3

Planificación

En este capítulo se propone una planificación del proyecto con el fin de organizar su estructura y exponer sus costes temporales y económicos aproximados necesarios para su realización.

3.1 Tareas

Tarea 1. Analizar como está formada la infraestructura, que componentes hardware y software la componen y cual es la función de cada uno de ellos.
En cuanto a la parte física se comprueban las especificaciones concretas del hardware de cómputo, almacenamiento y red. También como están organizados y estructurados tanto el sistema de almacenamiento y la red de la infraestructura. En la parte de software, se detallan las funciones de los principales programas y servicios que están instalados en el entorno.

Tarea 2. Analizar y seleccionar una herramienta de las disponibles en el mercado que se adapte a las necesidades del servicio que se quiere construir y a las características de la infraestructura. La herramienta seleccionada debe permitir reducir el coste y la complejidad de los trabajos de mantenimiento y administración del servicio a la vez que el usuario final lo utiliza de forma sencilla. En este proceso también se debe tener en cuenta la compatibilidad y eficiencia de la nueva herramienta con los componentes ya existentes en el entorno.

Tarea 3. Tarea que agrupa las tareas dedicadas al proceso de configuración de la infraestructura, configuración de la herramienta seleccionada y su instalación. Estas son las tareas 4, 5, 6, 7, 8, 9 y 10.

Tareas 4, 5, 6, 7, 8, 9 y 10. Comprobación de requisitos, preparación del entorno, establecimiento de parámetros configuración, despliegue de la plataforma sobre la infraestructura existente y configuración de la plataforma después del despliegue. Antes de realizar la ins-

talación de la nueva herramienta es necesario comprobar sus requisitos necesarios para que las capacidades del servicio final se adapten a las necesidades de uso (tareas 4 y 5). También se deben establecer los parámetros de configuración iniciales que se van a aplicar a la nueva plataforma (tarea 6). Durante el proceso de comprobación de requisitos puede surgir la necesidad de realizar cambios sobre las capacidades de la infraestructura y la configuración de los componentes ya existentes en el entorno inicial para que este se adapte a los requisitos de la nueva plataforma (tareas 7 y 8). Una vez el entorno está preparado para la herramienta pueda ser instalada entonces se efectúa el despliegue (tarea 9), posteriormente se configura y se comprueba el funcionamiento del nuevo servicio (tarea 10).

Tarea 11. Fin de la instalación y configuración de la plataforma. Marca el final del despliegue y configuración del nuevo servicio en la infraestructura.

Tarea 12. Diseñar una integración de la nueva plataforma con el sistema de autenticación de la UDC para que los usuarios finales del servicio se puedan autenticar sin necesitar nuevas credenciales. Para ello es preciso comprobar el método de acceso al directorio de usuarios de la UDC y la forma de conectarlo con la plataforma desplegada para, posteriormente, realizar un diseño de la solución. Este proceso requiere realizar una solicitud de acceso a los servicios internos de la UDC.

Tarea 13. Implementación y despliegue de la integración para la autenticación de usuarios con sus credenciales de la UDC. Durante este proceso puede ser necesario realizar cambios sobre la configuración de perfiles de usuarios que está establecida en la plataforma.

Tarea 14. Análisis del uso que harán los usuarios del servicio para establecer políticas sobre el uso de recursos. Para realizar este cálculo, primero se debe analizar el uso previo al despliegue del nuevo servicio que los usuarios hacen de la infraestructura y, después, estimar el uso que pueden llegar a realizar una vez el servicio sea accesible. Hay que tener en cuenta la cantidad de usuarios que lo utilizan, que lo van a utilizar y la cantidad de recursos que se emplean y que se van a emplear. Una vez obtenida una estimación, se realiza un diseño de las políticas que se van a aplicar.

Tarea 15. Diseño de un sistema de facturación/valoración de los recursos del servicio en base a las políticas de uso establecidas. Basándose en las políticas establecidas en la tarea 14, se debe pensar como se pueden aplicar sobre el servicio. Esto puede ser a través de una herramienta externa, en ese caso sería necesario realizar un desarrollo, o integrando la configuración en los parámetros de configuración de la plataforma.

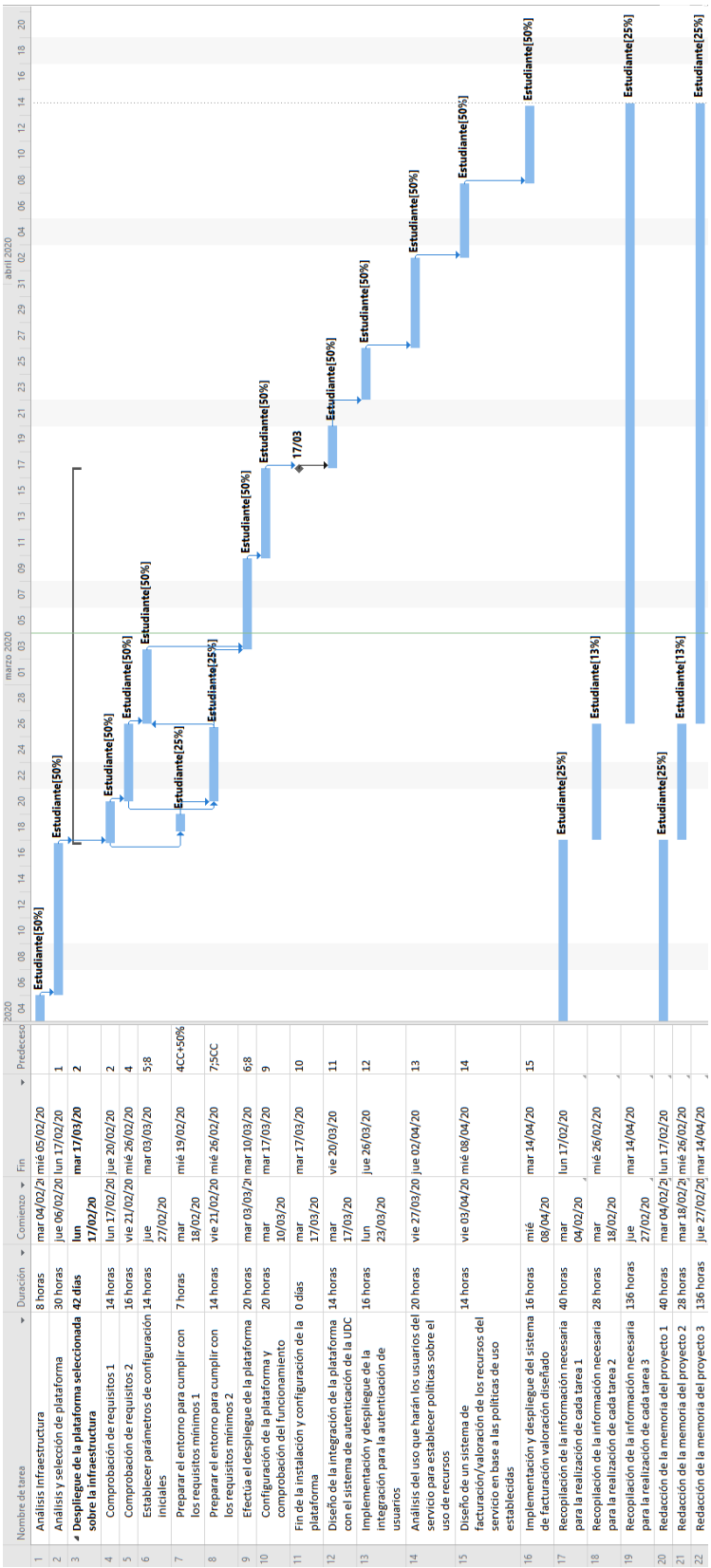
La intención de este sistema es limitar la cantidad de recursos que un usuario puede aprovisionar permitiendo aumentar la eficiencia de los recursos físicos reduciendo la cantidad de recursos ociosos.

Tarea 16. Implementación y despliegue del sistema de facturación/valoración. Para implementar este sistema puede que sea necesario realizar el desarrollo de una herramienta si se determina que no es posible establecerlo a través de los parámetros de configuración de la plataforma.

Tarea 17, 18 y 19. Recopilación de la información necesaria para la realización de cada tarea. La información de apoyo se debe obtener de documentaciones, artículos, vídeos o libros de fuentes fiables como empresas desarrolladoras de los productos utilizados o expertos especializados. El objetivo la recopilación de información es obtener conocimiento sobre las herramientas con las que se está trabajando para luego tener una base que facilite la realización de las tareas descritas. Esto se realiza desde el comienzo del proyecto hasta su finalización para tener claros los conceptos que se desarrollan y para conocer los detalles del trabajo que hay que realizar en cada tarea.

Tarea 20, 21 y 22. Redacción de la memoria del proyecto. Se escribe un documento con todos los detalles de todas las tareas realizadas durante el proyecto, incluyendo los cambios realizados en la infraestructura, las configuraciones establecidas y como se lleva a cabo cada proceso del proyecto. Su objetivo es transmitir el conocimiento adquirido durante el proyecto sobre como realizar el despliegue de una plataforma de virtualización y los beneficios que esta puede tener. La escritura de este documento se realiza a la vez que completa cada tarea para detallar los pasos realizados en cada caso, por lo que su duración es igual a la duración total de todo el proyecto.

La duración total del proyecto se estima en 101 días. teniendo en cuenta que el estudiante trabaja durante 4 horas diarias. El coste mostrado se refiere al coste correspondiente al estudiante si trabaja por 25 €/hora.



	Nombre de tarea	Duración	Comienzo	Fin	Predeceso
1	Análisis infraestructura	8 horas	mar 04/02/2	mié 05/02/20	
2	Análisis y selección de plataforma	30 horas	jue 06/02/20	lun 17/02/20	1
3	**Despliegue de la plataforma seleccionada sobre la infraestructura**	**42 días**	**lun 17/02/20**	**mar 17/03/20**	**2**
4	Comprobación de requisitos 1	14 horas	lun 17/02/20	jue 20/02/20	2
5	Comprobación de requisitos 2	16 horas	vie 21/02/20	mié 26/02/20	4
6	Establecer parámetros de configuración iniciales	14 horas	jue 27/02/20	mar 03/03/20	5;8
7	Preparar el entorno para cumplir con los requisitos mínimos 1	7 horas	mar 18/02/20	mié 19/02/20	4CC+50%
8	Preparar el entorno para cumplir con los requisitos mínimos 2	14 horas	vie 21/02/20	mié 26/02/20	7;5CC
9	Efectúa el despliegue de la plataforma	20 horas	mar 03/03/2	mar 10/03/20	6;8
10	Configuración de la plataforma y comprobación del funcionamiento	20 horas	mar 10/03/20	mar 17/03/20	9
11	Fin de la instalación y configuración de la plataforma	0 días	mar 17/03/20	mar 17/03/20	10
12	Diseño de la integración de la plataforma con el sistema de autenticación de la UDC	14 horas	mar 17/03/20	vie 20/03/20	11
13	Implementación y despliegue de la integración para la autenticación de usuarios	16 horas	lun 23/03/20	jue 26/03/20	12
14	Análisis del uso que harán los usuarios del servicio para establecer políticas sobre el uso de recursos	20 horas	vie 27/03/20	jue 02/04/20	13
15	Diseño de un sistema de facturación/valoración de los recursos del servicio en base a las políticas de uso establecidas	14 horas	vie 03/04/20	mié 08/04/20	14
16	Implementación y despliegue del sistema de facturación valoración diseñado	16 horas	mié 08/04/20	mar 14/04/20	15
17	Recopilación de la información necesaria para la realización de cada tarea 1	40 horas	mar 04/02/20	lun 17/02/20	
18	Recopilación de la información necesaria para la realización de cada tarea 2	28 horas	mar 18/02/20	mié 26/02/20	
19	Recopilación de la información necesaria para la realización de cada tarea 3	136 horas	jue 27/02/20	mar 14/04/20	
20	Redacción de la memoria del proyecto 1	40 horas	mar 04/02/2	lun 17/02/20	
21	Redacción de la memoria del proyecto 2	28 horas	mar 18/02/2	mié 26/02/20	
22	Redacción de la memoria del proyecto 3	136 horas	jue 27/02/20	mar 14/04/20	

Figura 3.1: Diagrama de Grantt sobre la planificación del proyecto.

	Comienzo	Fin
Actual	mar 04/02/20	mar 14/04/20
Previsto	mar 04/02/20	mar 14/04/20
Real	NOD	NOD
Variación	0d	0d

	Duración	Trabajo	Costo
Actual	100,75d	201,25h	5.031,25 €
Previsto	100,75d	201,25h	5.031,25 €
Real	0d	0h	0,00 €
Restante	100,75d	201,25h	5.031,25 €

Figura 3.2: Estadísticas sobre la planificación del proyecto.

3.2 Costes

Los principales costes del proyecto son aquellos relacionados con los trabajadores que lo llevan a cabo y las licencias necesarias para cada componente de VMware Cloud Foundation en la infraestructura[1].
Cada componente de VMware Cloud Foundation requiere su propia licencia[6]. Estos componentes son SDDC Manager, VMware vSphere, VMware vCenter, VMware vSAN, VMware NSX for vSphere y VMware vRealize Log Insight. El precio de cada licencia dependerá del número de CPUs físicas sobre las que se va usar esta plataforma por lo que, como en la infraestructura hay un total de ocho hosts con dos CPUs cada uno, el precio por cada componente es el siguiente:

- **SDDC Manager**: 18.000€[2] por CPU y 6.500€ anuales de soporte por cada CPU. El precio total de la licencia es de 288.000€ y 104.000€ anuales de soporte por 16 CPUs.

- **VMware vSphere**: 4.000€[3] por CPU. El precio total de la licencia es de 64.000€ por 16 CPUs y el precio anual por las tareas de soporte es de 16.000€.

- **VMware vCenter**: 6.000€[4] por una licencia que permite usar VMware vCenter sobre todos los hosts del entorno. El precio anual por las tareas de soporte es de 1.500€.

- **VMware vSAN**: 4.000€[5] por CPU. El precio total de la licencia es de 64.000€ por 16 CPUs y el precio anual por las tareas de soporte es de 16.000€.

[1] Los componentes que se especifican son aquellos que son obligatorios para desplegar VMware Cloud Foundation.
[2] Para la edición *Advanced* de VMware Cloud Foundation.
[3] Para la edición *Standard* de VMware vSphere.
[4] Para la edición *Standard* de VMware vCenter
[5] Para la edición *Advanced* de VMware vSAN.

- **VMware NSX for vSphere**: 5.300€[6] por CPU. El precio total de la licencia es de 84.400€ por 16 CPUs y el precio anual por las tareas de soporte es de 21.100€.
- **VMware vRealize Log Insight**: 1.500€ por CPU. El precio total de la licencia es de 24.000€ por 16 CPUs y el precio anual por las tareas de soporte es de 6.000€.

El precio total de todas las licencias necesarias para el entorno, teniendo en cuenta que hay 16 CPUs, sería igual a 530.400€, y el precio total por las tareas de soporte sería igual a 164.600€ anuales.

En caso de que ya estén instalados algunos de los componentes entonces solo se requieren licencias para aquellos componentes que aún no están en el entorno. En el caso del entorno inicial, los componentes que ya están instalados son VMware vSphere, VMware vCenter Server. Esto hace que el coste real para implementar VMware Cloud Foundation en el entorno sea igual a 460.400€, ya que solo son necesarias licencias para los componentes SDDC Manager, VMware vSAN, VMware NSX for vSphere y VMware vRealize Log Insight. El coste total de la instalación y mantenimiento de la plataforma VMware Cloud Foundation sobre la infraestrructura del CITIC es el siguiente:

- **Licencias**: 460.400€ en total.
- **Soporte**: 164.600€ anuales.
- **Sueldo empleado**: 5.031,25€ en total.

[6] Para la edición *Advanced* de NSX.

Capítulo 4

Metodología

En este capítulo se describirá el desarrollo del proyecto y las funcionalidades más destacadas de la solución. Para ello se describirán varios conceptos necesarios para entender las partes y estructura de VMware Cloud Foundation, los requisitos para implementar VCF en un entorno real, y finalmente el despliegue del producto sobre un entorno de prueba para demostrar sus características.

4.1 Conceptos

En este apartado se describen algunos conceptos que se deben tener claros para entender la estructura y arquitectura de los componentes de VMware Cloud Foundation.

4.1.1 Workload Domain

Un Workload Domain (WD) representa un bloque de recursos dentro del SDDC, formado por recursos físicos y virtuales, gestionados por los componentes de VCF. En cada WD se despliegan instancias de los componentes de VCF para controlar el acceso y uso de los recursos virtuales y físicos, estableciendo, además, una capa de seguridad sobre el WD. Esto permite que los recursos de cada WD se gestionen de forma separada. La función de un WD consiste en separar flujos de trabajo para determinar que recursos se dedican a la realización de determinadas tareas.

Management Domain

El Management Domain es el primer WD que se crea dentro del SDDC cuando se despliega VCF. Su finalidad es alojar todos los componentes de VCF que gestionan el propio Management Domain y al resto de WDs. Inicialmente, se despliegan las siguientes VMs de cada componente:

- Una VM de SDDC Manager.
- Una VM de VMware vCenter Server.
- Tres VMs de VMware NSX-T Manager Appliance.
- Dos VMs de VMware NSX-T Edge.

Al contener todas las instancias de los componentes dedicados a la gestión del SDDC, todas las tareas de administración suceden dentro de este WD. De esta forma, su ejecución está centralizada, es más segura y está mejor controlada, ya que lo hacen sobre un conjunto de recursos dedicados exclusivamente a ellas.

Virtual Infrastructure Domain (VI)

Este tipo de WD se crea manualmente y bajo demanda desde el Management Domain, para habilitar un entorno, cuyos recursos puedan ser usados por los usuarios mediante el despliegue de aplicaciones. Su configuración de hardware y lógica se especifican durante el proceso de creación, pudiendo establecer la cantidad de hosts, cantidad de almacenamiento, configuración de la red y políticas de rendimiento y disponibilidad, todo para satisfacer las necesidades del tipo de tareas que se van a realizar en él. Con la creación de un WD se generan las siguientes VMs:

- Una VM de VMware vCenter Server que se sitúa en el Management Domain.
- Tres VMs de VMware NSX-T Manager Appliance situadas en el Management Domain.
- Dos VMs de VMware NSX-T Edge.

Que ciertos componentes se sitúen en el Management Domain, permite separar las tareas de administración de un VI Domain de las aplicaciones y recursos de los usuarios, haciendo un entorno mejor organizado, más seguro y óptimo.

4.1.2 Arquitectura

VMware proporciona dos posibles modelos de arquitectura diferentes. Se utiliza uno u otro dependiendo del tamaño de la infraestructura sobre la que se va a desplegar VCF, y con cada modelo, se determina la forma en la que se agruparán y administrarán los recursos del SDDC.

Modelo estándar

Este modelo está pensado para entornos de tamaño medio/grande, con un mínimo de siete hosts. Está formado por un Management Domain y al menos un VI Domain. Esto implica que la ejecución de tareas dentro de un WD está limitada por los recursos que lo forman. Esto permite asignar roles a los recursos según las operaciones que se van a ejecutar sobre ellos, establecer un nivel de seguridad en cada WD y dedicar un conjunto de recursos a la ejecución de cierto tipo de operaciones. Así, el entorno es más eficiente, ya que se proporciona una forma de adecuar la configuración de los recursos de acuerdo con el uso que se va a hacer del servicio o servicios desplegados, minimizando además los cambios sobre la infraestructura física.

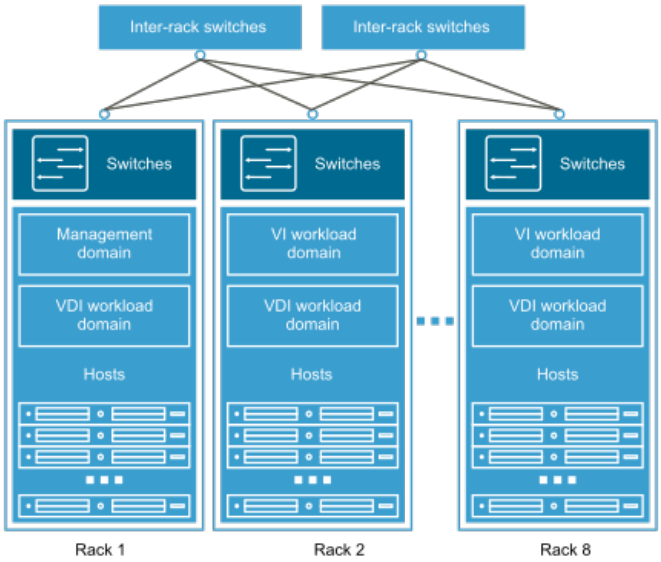


Figura 4.1: Esquema del modelo de arquitectura estándar.

Modelo consolidado

Este modelo está orientado a entornos de tamaño pequeño, con menos de siete hosts. Está formado por un único WD que cumple las funciones de un Management Domain y de un VI Domain, es decir, en él se colocan las instancias de los componentes dedicados a la gestión del SDDC[1] junto con las aplicaciones desplegadas para la realización de otro tipo de tareas. Así, a diferencia del modelo estándar, todas las operaciones se ejecutan dentro de un mismo entorno y sobre los mismos recursos. Internamente, las VMs se pueden colocar dentro de un grupo, llamado *resource pools*, en el que se puede establecer un límite de uso de recursos. Este modelo no aporta tantos beneficios como el modelo estándar, ya que todas las operaciones se

[1]Se despliega la misma cantidad de instancias que en el Management Domain.

realizan sobre los mismos recursos, y los niveles de control y seguridad son menores, por lo tanto su uso solo está recomendado para entornos de tamaño reducido.

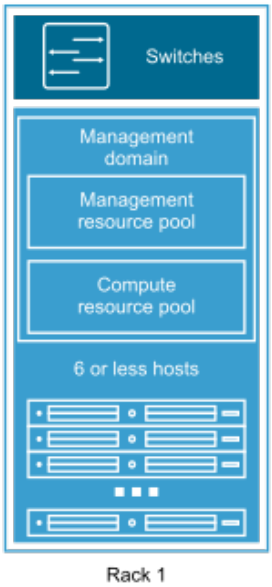


Figura 4.2: Esquema del modelo de arquitectura consolidado.

4.1.3 Clusters, zonas y distribución de un SDDC

Los recursos de un SDDC pueden estar distribuidos en diferentes localizaciones para proporcionar mayor disponibilidad y recuperación ante fallos. Estos recursos, se agrupan para formar una estructura que permite usar y gestionar los recursos disponibles de forma conjunta y dinámica.

Availability Zone, Region y Cluster

- Availability Zone (AZ): se llama AZ a un conjunto de recursos físicos que forman una infraestructura independiente, es decir, cada una tiene su propia fuente de energía, su sistema de refrigeración, su sistema de seguridad y su red, no compartidos con otra AZ, para evitar la propagación de fallos hacia otras AZs. Cuando existen varias AZs, se pueden usar de forma que cuando ocurre un fallo en una de ellas la carga de trabajo se distribuye a una segunda AZ y, así, minimizar el tiempo de caída del servicio. Dentro de una AZ se alojan uno o más WDs.

- Region: se llama Region a un conjunto de AZs situadas en una misma ubicación, es decir, las AZs de una Region están situadas próximas entre sí. Estas AZs deben tener al menos una latencia de 5 ms entre ellas. Dentro de un SDDC pueden existir varias

Regions pero estas se sitúan en ubicaciones más distantes, la latencia debe ser de al menos 150 ms. Esta estructura permite ofrecer los servicios de un SDDC en diferentes ubicaciones, a la vez que se aumenta su disponibilidad y recuperación ante fallos.

- Cluster: un cluster de VMware vSphere es una agrupación de hosts. A las instancias desplegadas sobre ellos, se les aplica una configuración de disponibilidad con el componente VMware vSphere, permitiendo determinar como se restablecen las instancias cuando ocurre un fallo dentro del cluster. Un cluster se sitúa dentro de un WD, por lo tanto, sus recursos estarán limitados por el alcance del WD.

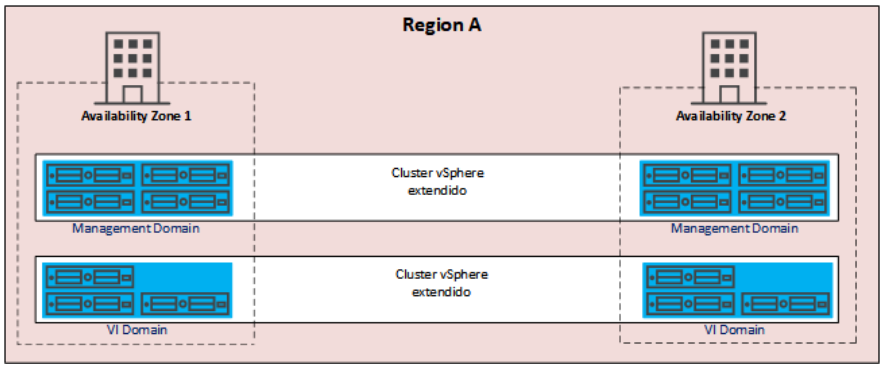


Figura 4.3: Ejemplo de un SDDC con dos Regions y una AZ en cada uno.

En la figura anterior se describe el esquema de un SDDC compuesto de una Region. Dentro de esta, existen dos AZ, AZ1 y AZ2. Cada una de las AZs contiene dos WD, un Management Domain desde donde se administra el SDDC, y un VI Domain donde se realizan las operaciones del SDDC. Como se mencionaba anteriormente, las instancias situadas en una AZ pueden migrar de una ubicación a otra en caso de fallo de los recursos físicos. Para ello, el WD donde se encuentran esas instancias debe estar extendido en las dos AZs. En la imagen, el Management Domain está formado por ocho hosts, repartidos en las AZs, los cuales están agrupados dentro del mismo cluster de VMware vSphere, por lo tanto, los componentes cuyas instancias estén situadas en este cluster se podrán migrar entre los 8 hosts. Estas migraciones se realizan en función de la configuración de disponibilidad establecida en los componentes VMware vSphere y VMware vSAN. Así, cuando los hosts de AZ1 sufren una caída, la AZ2 seguiría activa y las instancias situadas en AZ1 migrarían a AZ2 para continuar la disponibilidad del servicio, todo esto de forma automatizada, dinámica y transparente para el usuario. Lo mismo sucedería con el VI Domain[2].

[2]Se puede encontrar una descripción más detallada de esta estructura en el siguiente enlace https://docs.vmware.com/en/VMware-Validated-Design/6.0/introducing-vmware-validated-design/GUID-661B1CE3-1F74-4E00-80F3-0F5EA39528CD.html

4.2 Requisitos

En este apartado se describe aquello que debe cumplir la infraestructura física para que los componentes de VMware Cloud Foundation funcionen de forma adecuada y que la configuración y mantenimiento de los componentes físicos sea simple a la hora de expandir el entorno.

4.2.1 Cómputo

Hosts ESXi

Para realizar el despliegue del primer WD (el Management Domain) se requieren al menos cuatro[3] hosts ESXi con al menos un 128 GB de memoria RAM y un disco de arranque de 32 GB cada uno[4]. Para cada WD adicional solo se requiere un mínimo de tres hosts y la cantidad de memoria RAM depende de la finalidad del WD, por lo tanto para implementar el modelo de arquitectura estándar se requieren al menos siete hosts ESXi. Cada uno de los hosts debe tener al menos dos interfaces de red físicas (NIC) que soporten al menos 10 Gbit/seg de velocidad.

4.2.2 Almacenamiento

En el Management Domain es obligatorio el uso de un *datastore* de VMware vSAN, este necesita al menos tres hosts con recursos de almacenamiento para funcionar[5]. Se debe aplicar la configuración All-Flash con discos SSD. Basándose en los perfiles que VMware establece para su producto vSAN Ready Node[7], cada host debe tener al menos un grupo de dos discos donde la cantidad de almacenamiento para la capa de capacidad debe ser de 4 TB y para la capa de caché de 200 GB. VMware vSAN soporta discos con adaptadores SAS, SATA o SCSI y estos pueden estar configurados en modo *pass-through* o RAID 0. En cuanto a esto, es preferible que los discos se configuren en modo *pass-through* ya que permite que estos se puedan gestionar de forma independiente, sin tener que apagar los hosts cuando sea necesario retirar o añadir discos. Para WD adicionales se puede utilizar almacenamiento NFS en lugar de un *datastore* de VMware vSAN, aunque la solución de VMware aporta mayor rendimiento y simplifica la administración de esta parte de la infraestructura física.

[3] Se reserva la cuarta parte de los recursos para que el *management domain* permanezca activo en caso de caída de alguno de los hosts.

[4] Según la configuración establecida para el producto vSAN ReadyNode [7]

[5] VMware vSAN requiere un mínimo de tres hosts mientras que el Management Domain requiere un mínimo de cuatro hosts.

4.2.3 Red

Switch Top Of Rack

Los hosts están colocados en racks, en un rack puede haber hosts pertenecientes a distintos WD. Para favorecer la alta disponibilidad y tolerancia a fallos de la infraestructura física, un rack debe tener dos switches Top Of Rack (TOR) y cada host debe tener una interfaz conectada a cada uno de ellos, una capa superior de switches conecta los switches TOR entre sí. Todas las conexiones de la red física deben soportar *Jumbo frames* (MTU hasta 9000 Bytes), etiquetado *Quality of Service* (QoS) de tráfico y el etiquetado VLAN, todo para dar soporte a las subredes del SDDC[6]. Todas las conexiones físicas deben tener, al menos, 10 Gbit/seg de velocidad.

Servicios

En el SDDC se deben habilitar varios servicios requeridos por los componentes de VMware Cloud Foundation para su correcto funcionamiento.

- DNS: servidor de nombres para resolver todas las direcciones IP y *hostnames* de los componentes del SDDC.
- DHCP: servidor para asignar de forma automática una dirección IP a los hosts que forman el SDDC.
- NTP: servidor de tiempo para sincronizar la hora de todos los componentes del SDDC.
- Router: se requiere para enrutar el tráfico que emiten todas las instancias del SDDC y para dar acceso a redes externas. Debe soportar enrutamiento dinámico BGP y debe tener configuradas las subredes y VLANS que se vayan a utilizar en la infraestructura.
- SMTP: servidor de correo utilizado por el componente VMware vRealize Automation.
- Active Directory: servidor de usuarios y grupos de usuarios que el SDDC utiliza como fuente para configurar el acceso a cada parte de la infraestructura virtual.
- Certificate Authority: se debe configurar una autoridad certificadora que genere certificados firmados para cada uno de los componentes de VMware Cloud Foundation. Permite establecer conexiones seguras cuando se accede a los componentes.

[6]Para el Management Domain, las subredes cuya VLAN debe ser configurada en la red física son la subred Management para tareas de administración, la subred dedicada a VMware vSAN, la subred dedicada a overlay y la subred dedicada a VMware vSphere vMotion.

4.3 Prueba de concepto

Para no afectar al funcionamiento de los trabajos que se llevan a cabo en el CITIC, el proyecto se lleva a cabo en un entorno aislado en el cual se despliegan todos los componentes de VCF, con el fin mostrar y probar las capacidades y características de VMware Cloud Foundation. El proceso se realizará siguiendo la metodología Scrum, donde en cada ciclo se realizará el despliegue de uno o varios componentes y luego se revisará su configuración y funcionamiento. Primero se instalarán los componentes base de VMware Cloud Foundation[7] usando el programa VMware Lab Constructor (VLC) v4.0.1[8]. Posteriormente se instalarán los componentes de la suite VMware vRealize, uno dedicado a la gestión de usuarios del SDDC y otro que proporciona un servicio de aprovisionamiento, llamados Workspace One Access y vRealize Automation respectivamente. Finalmente, se comprobará el funcionamiento general del SDDC y las posibilidades que ofrece el servicio Cloud desplegado.

4.3.1 Preparación

En esta sección se describen los elementos y servicios que serán usados por los componentes de VMware y que son necesarios para su correcto funcionamiento.

VMware Lab Constructor v4.0.1

El programa VMware Lab Constructor v4.0.1 (VLC), es una herramienta desarrollada por trabajadores de VMware con la cual se crea un entorno embebido dentro de un host físico. Este entorno se compone de cuatro hosts con el hipervisor ESXi, en forma de VMs. Dentro de estos hosts, VLC despliega los componentes de VCF.

[7] Los componentes base de VCF son VMware vSphere, VMware vSAN y VMware NSX-T

[8] Herramienta que permite crear un generar de forma automatizada un entorno embebido para probar las funcionalidades de VMware Cloud Foundation.

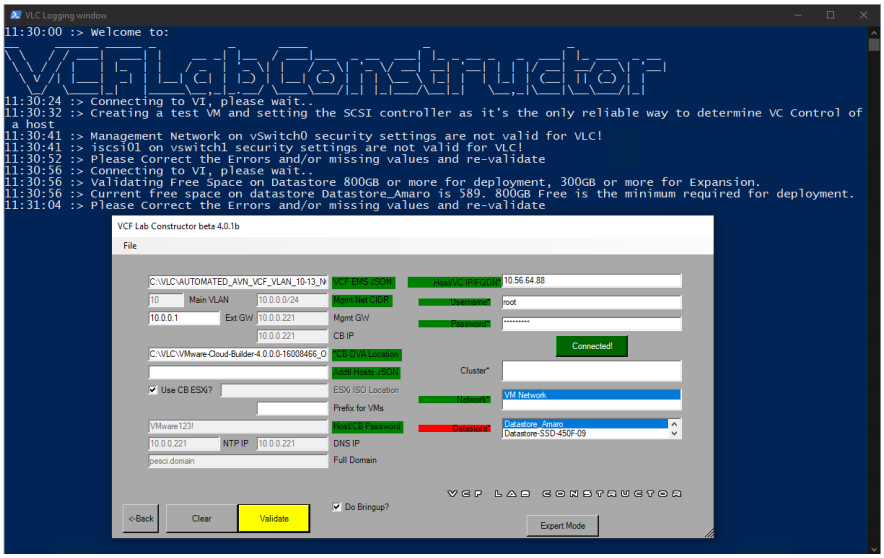


Figura 4.4: Herramienta VMware Lab Constructor v4.0.1b

Host ESXi

El host sobre el que VLC realiza la instalación del entorno se trata de un servidor con el hipervisor ESXi instalado. Este servidor cuenta con una memoria RAM de 192 GB, una CPU de 28,8 GHz y está conectado a un datastore formado por discos SSD y con una capacidad de 2 TB. Además, incorpora dos interfaces de red. La primera interfaz se conecta a una red para acceder al datastore, mientras que la segunda, se conecta a una red utilizada para acceder de forma remota al servidor y a otra red dedicada a comunicar los componentes desplegados dentro del host.

Servicios

Los servicios externos requeridos por VCF se sitúan dentro del mismo servidor físico. Estos están colocados en una VM con el sistema operativo Windows Server 2016, el cual incluye DNS, NTP, SMTP, y los servicios Active Directory (AD) y Certificate Authority (CA). También incorpora un router en forma de VM, con el sistema operativo VyOS, que también cuenta con servicio DHCP. El servidor DNS utiliza el nombre de dominio *pesci.domain*. El almacén Active Directory sustituye al servicio de autenticación de la UDC para poder manejar cuentas de usuarios sin causar conflictos en el funcionamiento de los servicios en producción.

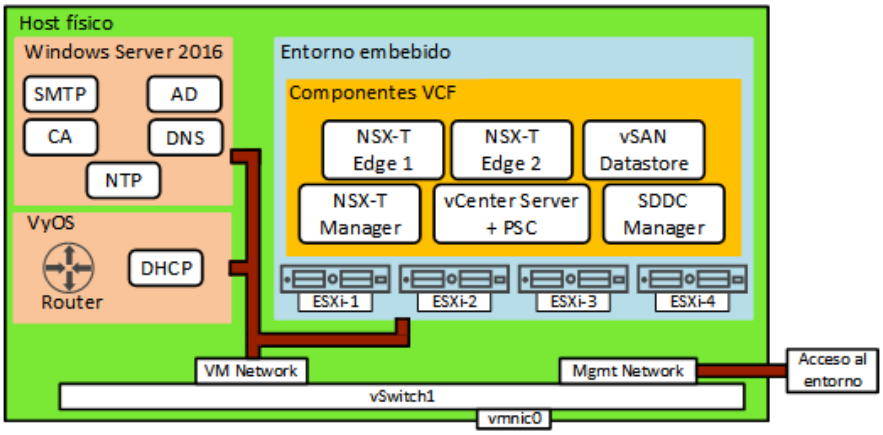


Figura 4.5: Elementos desplegados en el host físico.

En la imagen anterior, se muestra el entorno embebido y las VMs que VLC genera dentro del host físico, junto a los servicios necesarios para el correcto funcionamiento de VCF. También se muestran las dos redes a las que se conecta la interfaz *vmnic0* del host. *VM Network* comunica a todos los elementos desplegados y representa la red física del entorno. La red *Mgmt Network* se utiliza para acceder al host de forma remota.

4.3.2 Diseño y configuración del Management Domain

En esta sección se describen las funciones y configuración de los componentes desplegados en el entorno de pruebas con la ayuda de VLC.

Diseño de VMware vCenter Server

El componente VMware vCenter Server es el punto de acceso y de control de todas las VMs localizadas en los hosts ESXi bajo su dominio. VMware vCenter Server funciona sobre una VM situada en el Management Domain. Esta instancia de vCenter Server contiene un dominio con un cluster vSphere que agrupa a los cuatro hosts ESXi que forman el Magement Domain. Estos hosts se denominan respectivamente *esxi-1*, *esxi-2*, *esxi-3* y *esxi-4*, y cada uno cuenta con 64 GB de memoria RAM y 19,9 GHz de CPU. Desde VMware vCenter Server el administrador gestiona los recursos de las VMs de cada componente, monitoriza los recursos, administra la creación y asignación de roles, permisos y usuarios, gestiona los grupos de discos que forman el *datastore* de VMware vSAN, determina las redes a las que se conecta cada componente, establece la configuración de disponibilidad y recuperación ante fallos proporcionada por VMware vSphere, en definitiva, VMware vCenter Server es el punto desde donde se controla y administra el uso de recursos por parte de las VMs desplegadas. Además, integra el componente PSC, el cual controla la identidad y permisos de los administradores y aplica-

ciones que acceden a VMware vCenter, y gestiona el almacenamiento de licencias de VCF. El acceso a VMware vCenter Server se hace a través del componente vSphere Web Client.

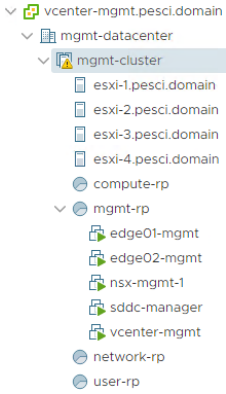


Figura 4.6: Dominio y cluster vSphere del Management Domain.

En la imagen anterior se muestra el dominio (*vcenter-mgmt.pesci.domain*), de la instancia de VMware vCenter Server, y el cluster vSphere (*mgmt-cluster*) donde se alojan los componentes del Management Domain. Este cluster incluye los cuatro hosts ESXi y cuatro *resource pools*, uno de ellos contiene las VMs de los componentes dedicados al Management Domain.

Diseño almacenamiento VMware vSAN

Los hosts del Management Domain utilizan como almacenamiento un *datastore* del componente VMware vSAN. Está formado por 16 discos SDD agrupados en cuatro grupos con configuración All-Flash, cada grupo está asociado a un host. Para mantener la disponibilidad de los ficheros almacenados en el *datastore*, se establece la opción *Failures-To-Tolerate* (FTT) igual a uno. De esta forma, VMware vSAN mantiene dos copias de los archivos generados por las VMs y las coloca en grupos de discos distintos, de forma que si ocurre un fallo en alguno de los hosts las VM seguirán teniendo acceso a sus archivos. Esta configuración equivale a tener un sistema de almacenamiento RAID 1, pero con la ventaja de que no se ha modificado la configuración del hardware y, si fuera necesario, se podría aumentar el número de réplicas simplemente editando el valor de FTT desde el portal de VMware vCenter Server. Como se muestra en la siguiente figura, VMware vSAN mantiene una copia del mismo archivo en dos hosts/grupos de discos diferentes, mientras la configuración física de cada grupo de discos es de tipo RAID 0. Las máquinas virtuales acceden al *datastore* a través de una subred que utiliza su propia VLAN y a la que todos los hosts están conectados.

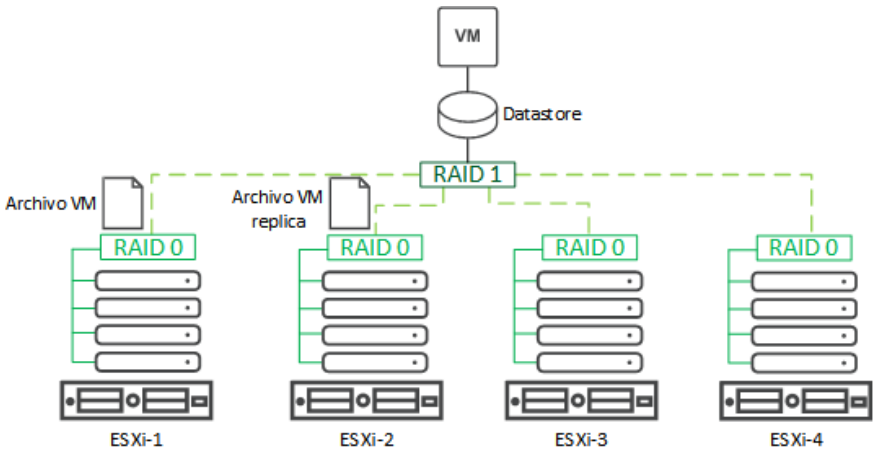


Figura 4.7: Ejemplo de como se almacena un archivo con VMware vSAN y FTT igual a uno

Utilizar el sistema de almacenamiento de VMware vSAN supone una gran mejora respecto al sistema de almacenamiento basado en LUNs, utilizado actualmente en el CPD del CITIC. VMware vSAN monitoriza los dispositivos de almacenamiento y configura la redundancia de los archivos de forma dinámica y sencilla, permitiendo establecer una configuración específica según sea necesario, sin modificar los dispositivos físicos de almacenamiento. Con el sistema basado en LUNs, es obligatorio modificar la estructura y configuración de los dispositivos físicos cada vez que se quiera establecer una configuración de redundancia diferente en el sistema de almacenamiento, lo cual supone un gran coste para el administrador y un aumento de los riesgos. Si tomamos el ejemplo de la figura anterior, la redundancia el sistema gestionado por VMware vSAN, con FTT igual a 1, podría ser aumentada estableciendo la opción de configuración FTT igual a 2. Así, se crearía una nueva copia del archivo en un tercer grupo de discos, mientras la configuración física se mantiene igual.

Diseño cluster VMware vSphere

Como ya se ha mencionado, los cuatro hosts desplegados para el Management Domain están agrupados en un cluster de VMware vSphere. Gracias a dos funcionalidades de este componente, se establece una configuración para mantener activas las VMs desplegadas[9] dentro de este cluster. Entonces, VMware vSphere se encarga, de forma automatizada, de balancear el consumo de recursos y de recuperar el servicio de las VMs cuando alguna sufre un fallo. Estas funciones de VMware vSphere son:

- vSphere High Availability: establece una cantidad de recursos que se reserva de los disponibles en el cluster vSphere, y se encarga de reiniciar una VM cuando deja de

[9]Las VMs a las que se refiere son las instancias de cada componente de VCF.

estar operativa. Para este cluster se establece una reserva el 25% de la CPU total y el 25% de la memoria RAM total. De esta forma, se asegura que una cuarta parte de los recursos disponibles están reservados para reiniciar, en un host diferente, una VM que ha dejado de funcionar.

- vSphere DRS: se encarga de migrar VMs de un host a otro dentro del cluster vSphere,con el objetivo de balancear la carga de trabajo entre los hosts disponibles. Usando este servicio se garantiza que cada VM obtiene la capacidad necesaria para funcionar correctamente, y aumenta la eficiencia del cluster al hacerse un mejor uso de sus recursos. Para realizar las migraciones entre hosts, vSphere DRS utiliza la funcionalidad vMotion, el cual permite mover una VM de un host a otro manteniendo el estado en el que se encontraba, y manteniendo activo el servicio de la VM. Por ejemplo, si el consumo de recursos de un host está alrededor del 100%, vSphere DRS lo detecta e inicia la migración de la VM mediante vMotion, a otro host con recursos disponibles.

Combinando estas dos funcionalidades, las tareas de mantenimiento se reducen ya que es VMware vSphere quien, de forma automatizada y transparente, se encarga de monitorizar el estado de VMs y hosts, de optimizar el uso de recursos y de asegurarse de que existen suficientes recursos para la ejecución de todos los flujos de trabajo.

Diseño de red para el cluster vSphere

A parte de controlar la disponibilidad de los recursos, VMware vSphere también se encarga de gestionar las redes a las que se conecta cada VM, permitiendo separar cada tipo de tráfico en subredes y asignarles unas propiedades específicas. Para llevar esto a cabo y que las VMs puedan conectarse a la red externa y comunicarse con el resto de VMs, dentro del cluster vSphere se crea un vShpere Distributed Switch (vDS), en el cual se configuran puertos a los que se conectan las VMs alojadas en el cluster vSphere.

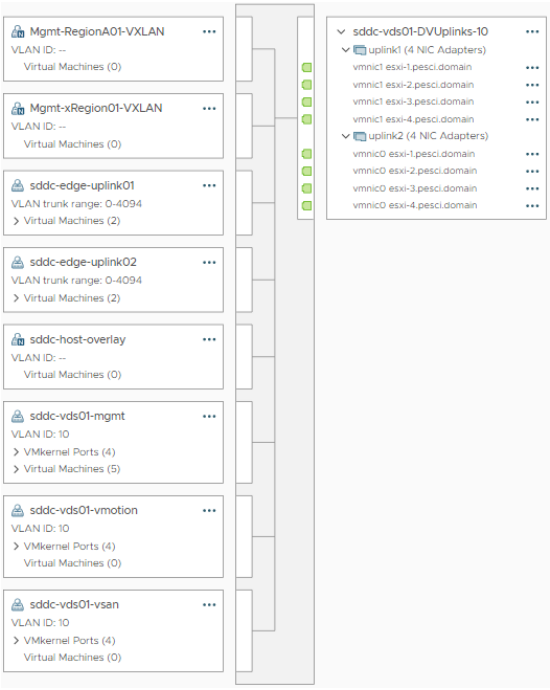


Figura 4.8: Contenido de vSphere Distributed Switch *sddc-vds01*.

Como se muestra en la imagen anterior, el vDS creado para el cluster vSphere del Management Domain contiene varios puertos, donde hay VMs conectadas, y dos interfaces uplink (*sddc-vds01-DVUplinks-10*). Estas dos interfaces, *uplink1* y *uplink2*, representan las interfaces de red físicas de cada host y son las que dan salida al tráfico de las VMs hacia la red física del entorno. Cada uno de los puertos tiene una función específica, estos son, *sddc-vds01-mgmt*, dedicado al tráfico de configuración y gestión que los componentes de VCF envían entre sí, *sddc-vds01-vmotion*, dedicado al tráfico de las migraciones de VMs entre hosts llevadas a cabo por la funcionalidad vMotion, *sddc-vds01-vsan*, usado por las VMs para acceder al datastore de VMware vSAN el cual es el sistema de almacenamiento del entorno, *sddc-edge-uplink01* y *sddc-edge-uplink02*, puertos usados por los componentes de VMware NSX-T para dar salida, hacia la red física, al tráfico de las redes virtuales que gestiona este componente de VCF. Los demás puertos que se muestran en la imagen son generados de forma automática por VMware NSX-T. En la configuración de cada puerto, se establece la VLAN que se asigna a su tráfico, las interfaces uplink por las que se transmite su tráfico hacia la red física, cómo se balancea la carga entre cada interfaz uplink, y la prioridad que se asigna a su tráfico respecto al resto de puertos. Los puertos, cuyo tráfico tiene mayor prioridad son, *sddc-vds01-vsan* y *sddc-vds01-vmotion*, para asegurarse de que obtienen el suficiente ancho de banda y así facilitar la transmisión de archivos de gran tamaño.
De esta forma, cada subred utilizada por los componentes de VCF es asociada con un puerto

del vDS, por lo tanto, las propiedades del tráfico de cada subred son configuradas a través de VMware vSphere. Esto, simplifica el proceso administración y configuración de las redes del entorno, ya que una vez configurados los dispositivos de red físicos, el router VyOS en este caso, con las direcciones IP, las etiquetas VLAN y MTU correspondientes a cada subred, la monitorización de la red y la configuración de la calidad del servicio se realizan desde VMware vSphere.

Diseño de la red del SDDC con VMware NSX-T

En el SDDC existe una red virtual que se define mediante software, también se le llama Software Defined Network (SDN). Esta red virtual está desacoplada de la infraestructura física, lo cual permite modificar su configuración sin necesidad de realizar cambios en la infraestructura de red ni en la configuración de los dispositivos de red físicos. Además, al estar definida por software, permite implementar diferentes configuraciones de red, mejorando y simplificando la administración y seguridad de las nuevas redes que se añaden al entorno. El componente encargado de mantener las redes virtuales del SDDC es VMware NSX-T.

En el Management Domain se despliega una instancia de NSX-T Manager y dos instancias del componente NSX-T Edge.

La virtualización de la red con VMware NSX-T se basa en dos componentes, Transport Zone (TZ) y Segment.

- Transport Zone: se trata de un contenedor dentro del cual se definen Segments. A una TZ se conectan TNs[10] para acceder a los Segments. Cada TN puede estar conectado a varias Transport Zones.

- Segment: se trata de un dominio de broadcast de capa 2 (una subred) que forma parte de una TZ. Las VMs se conectan a los Segments para acceder a la subred.

Una TZ se extiende en diferentes hosts que pueden estar situados en la misma red a nivel físico, o en distintas partes de la infraestructura del SDDC. Los hosts que estén conectados a una TZ tendrán acceso a los Segments (cada Segment equivale a una subred) generados en esa TZ. Así, se hace posible la creación de redes accesibles desde cualquier parte de la infraestructura del SDDC sin necesidad de modificar los dispositivos de red físicos. En el entorno, existen dos TZs. Una de ellas, la TZ *mgmt-domain-m01-overlay-tz*, contiene dos Segments, *mgmt-Region01A-VXLAN* y *mgmt-xRegion01-VXLAN*, los cuales son utilizados para conectar las instancias de los componentes de VMware vRealize Suite. La otra TZ disponible, *sfo01-m01-edge-uplink-tz* contiene otros dos Segments, utilizados para dar salida hacia el router VyOS al tráfico que circula por la TZ anterior (*mgmt-domain-m01-overlay-tz*). Para que el tráfico de cada Segment

[10] Los Transport Nodes son los hosts físicos y cada instancia de VMware NSX-T Edge.

pueda circular por la red física de la infraestructura, VMware NSX-T lo encapsula cuando sale de un host para que este pueda llegar al host destinatario. Los encargados de gestionar el enrutamiento entre Segments y hacia la red externa son las instancias de NSX-T Edge. Para ello, internamente forman una estructura de routers virtuales que a parte de realizar las tareas de enrutamiento, proporcionan servicios de red como NAT, Load Balancing, DNS, DHCP, VPN y Firewall, y mantienen rutas redundantes hacia el dispositivo físico de red.

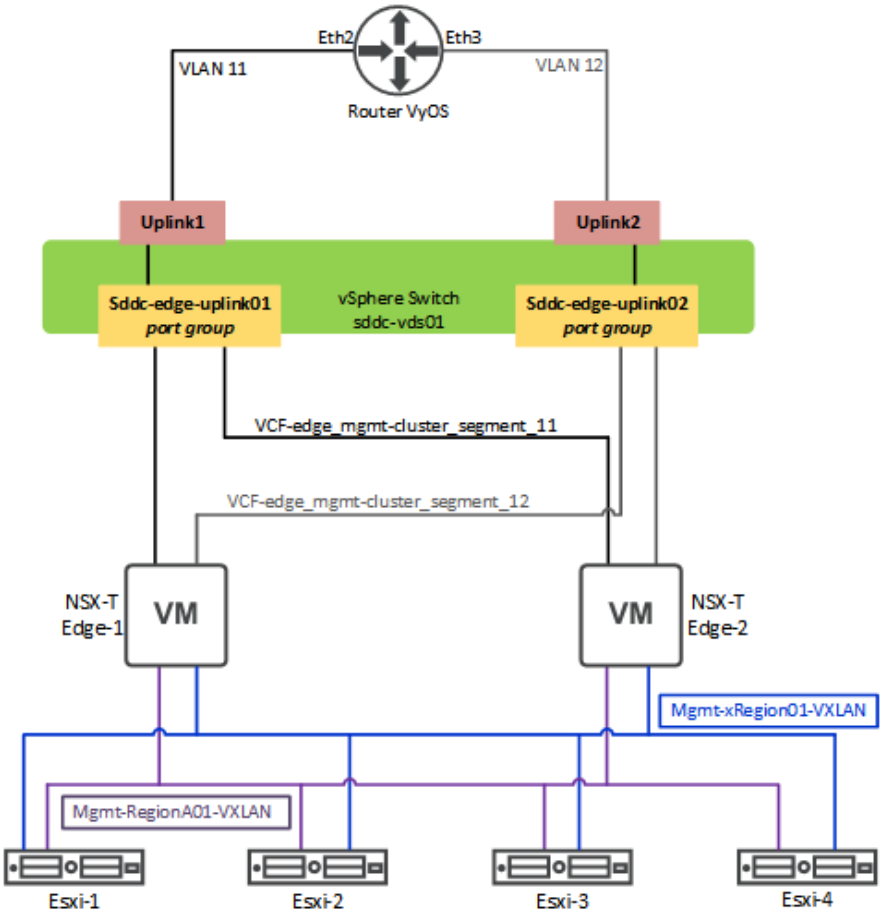


Figura 4.9: Segments a los que se conecta cada nodo de VMware NSX-T y como acceden a la red física.

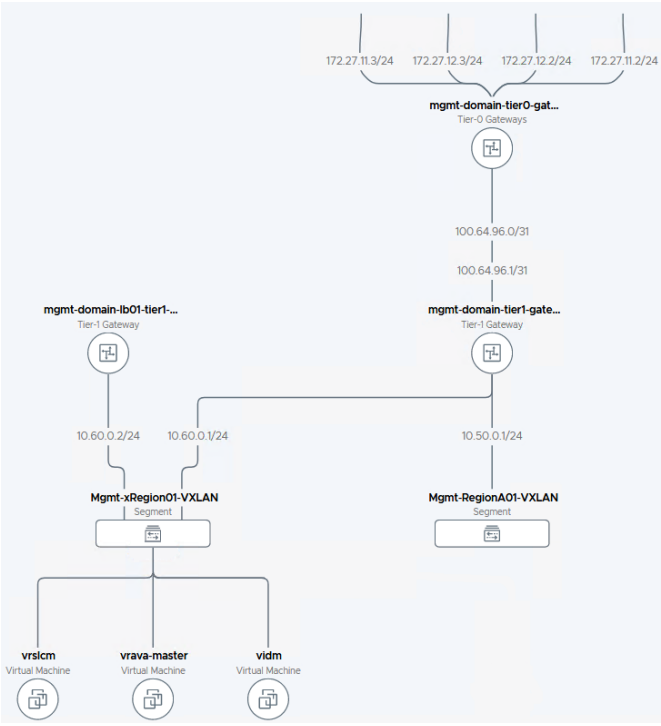


Figura 4.10: Topología virtual de VMware NSX-T

En la primera imagen (Figura 4.9), se muestra como cada host se conecta a los dos Segments disponibles para que las VMs que se residen en ellos puedan acceder a la red. Como ya se ha comentado, las VMs de NSX-T Edge enrutan el tráfico de esos Segments hacia la red física, a través del vDS desplegado en VMware vSphere. En la segunda imagen (Figura 4.10), se muestra la misma estructura pero desde el punto de vista interno de VMware NSX-T. En ella se aprecian los dos Segments donde uno de ellos tiene tres VMs conectadas (componentes de VMware vRealize Suite), y tres routers virtuales (dos Tier-1 y un Tier-0). Los routers Tier-1 proporcionan servicios de red, *mgmt-domain-lb01-tier1* proporciona un balanceador de carga para los componentes de VMware vRealize Suite, y enrutamiento entre Segments, mientras que el router Tier-0 se encarga de dirigir el tráfico hacia la red física (router VyOS), a través de cuatro conexiones que se corresponden con las que se conectan al vDS que se muestra en la figura 4.9. Para que el router VyOS tenga conocimiento de las redes virtuales existentes, las instancias de NSX-T Edge las anuncian mediante el protocolo de enrutamiento dinámico BGP.

Usando VMware NSX-T, el administrador puede gestionar y crear redes para ser consumidas por los usuarios de la plataforma. La creación de estas redes virtuales se hace bajo demanda y no requiere ninguna configuración adicional en los dispositivos de la red física. Su gestión se realiza siempre desde VMware NSX-T, el cual permite monitorizarlas, controlar su segu-

ridad y establecer servicios dedicados a estas redes virtuales. Además, permite extender una red virtual sobre diferentes redes físicas, permitiendo acceder a las VMs conectadas a esa red virtual desde diferentes puntos del SDDC, y migrar esas VMs de una localización a otra sin necesidad de cambiar su configuración, ni de la VM ni de la red física. En la infraestructura actual del CITIC todo esto no es posible, las redes que se crean dentro del entorno de VCF deben configurarse previamente sobre la red física, y todos los servicios de red necesarios deben ser proporcionados también desde dispositivos físicos, es decir, no existe una plataforma que permita gestionar las redes de la infraestructura de una forma dinámica y sin un alto coste en tiempo y riesgos.

4.3.3 Operaciones de la Arquitectura

En este punto ya se ha formado el SDDC, la configuración de la infraestructura física y de todos los componentes de VCF está preparada para desplegar la plataforma que habilite el servicio Cloud. Este último paso se completará con los servicios que proporciona VMware con los productos que agrupa en VMware vRealize Suite, estos proporcionarán un servicio de autenticación centralizado para los usuarios y servicio de aprovisionamiento de recursos. Se utilizarán tres componentes de VMware vRealize Suite, estos son vRealize Suite Lifecycle Manager (vRSLCM), Workspace One Access (WSA) y vRealize Automation (vRA). El despliegue de estos servicios dentro del entorno será iniciado desde el componente SDDC Manager y, para aprovechar las ventajas de VMware NSX-T y las redes virtuales existentes, utilizarán como red de acceso el Segment *mgmt-xRegion01-VXLAN*.

vRealize Suite Lifecycle Manager

vRSLCM es el primer componente que se instala (este proceso se hace desde SDDC Manager) ya que es el encargado de gestionar todo lo relacionado con el resto de productos de VMware vRealize Suite. Como su nombre indica, su función es gestionar el ciclo de vida de los servicios de VMware vRealize Suite en el SDDC, incluyendo su despliegue, actualizaciones y gestión de las credenciales de administración, certificados y licencias, por lo tanto, este componente permite al administrador controlar de forma centralizada la configuración y seguridad de los servicios dedicados a las operaciones del SDDC. Para llevar a cabo sus funciones, vRSLCM debe mantener una comunicación con la instancia de VMware vCenter Server desplegada en el Management Domain.

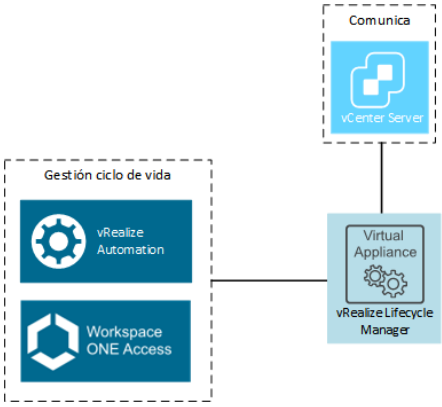


Figura 4.11: Componentes con los que se comunica vRSLCM.

Durante el despliegue de WSA y vRA, desde vRSLCM se establece su configuración, indicando la licencia, credenciales del administrador, direcciones IP, configuración DNS y NTP, y certificados para que los usuarios puedan acceder de forma segura a través del navegador[11]. Además, se debe elegir la ubicación donde se van a desplegar las VMs de estos servicios, es decir, el dominio de VMware vCenter Server, el cluster vSphere, la red y el datastore para el almacenamiento. En el entorno de pruebas, de cada servicio se crea una instancia en el Management Domain, se colocan en el cluster vSphere (Diseño cluster VMware vSphere), utilizan el datastore de VMware vSAN (Diseño almacenamiento VMware vSAN) y están controladas por la instancia de VMware vCenter Server (Diseño de VMware vCenter Server). Como ya se ha mencionado, las instancias se conectan a un Segment controlado por VMware NSX-T (como se muestra en la figura 4.10) para poder hacer uso de sus servicios de red.

[11]El certificado de cada aplicación es generado manualmente desde la CA y luego subido a vRSLCM, que en este caso es la VM con Windows Server 2016.

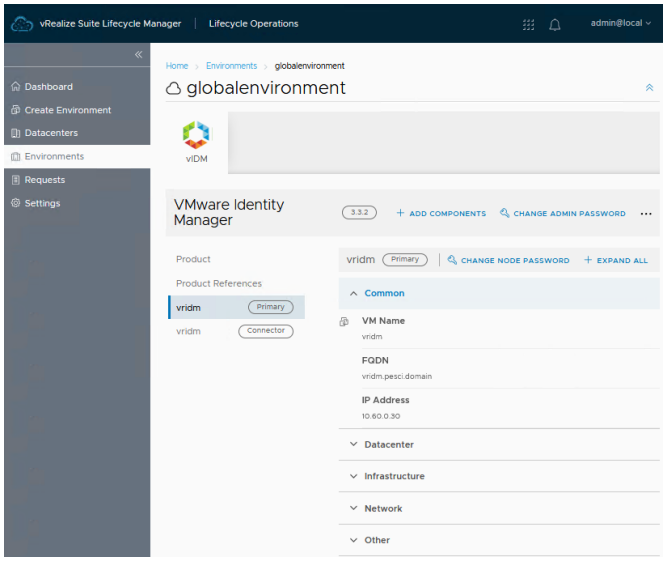
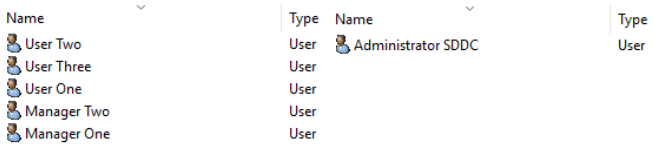


Figura 4.12: Apartado donde se muestra la configuración de la instancia de WSA en vRSLCM.

Workspace One Access

WSA es el componente de VMware vRealize Suite que se integra con un directorio de usuarios para proporcionarles acceso a las aplicaciones que se despliegan en el entorno, vRA en este caso. Así, en el entorno de producción, WSA se utilizaría para que los usuarios del SDDC se pudieran conectar utilizando sus credenciales de la UDC, ya que estaría conectado al directorio de la universidad. En el entorno de pruebas, se integra con el directorio de usuarios Active Directory situado en la VM con Windows Server 2016. Este Active Directory contiene perfiles de usuarios y grupos de usuarios organizados en unidades organizativas, los perfiles de usuario se añaden a grupos de usuarios, y la creación y mantenimiento de sus credenciales se realiza desde el propio Active Directory. Desde WSA se seleccionan los usuarios y grupos de usuarios que se quieran sincronizar para que estén disponibles en el SDDC y, posteriormente, desde cada aplicación se determina el nivel de acceso y permisos para cada usuario. Como norma general se deben asignar permisos a grupos de usuarios y no a perfiles individuales, de esta forma se reduce el tiempo de gestión y se simplifica la estructura, ya que para asignar nuevos permisos a un usuario solo sería necesario añadirlo al grupo correspondiente. En Active Directory se han configurado varios usuarios que se sincronizan en WSA. Estos se utilizarán para mostrar las funcionalidades de vRA como si se tratase del entorno de producción con perfiles de usuarios de la UDC. Desde WSA se seleccionan aquellas unidades organizativas que se quieren sincronizar. Cada unidad contiene usuarios y grupos de usuarios, los usuarios que harán uso del servicio de aprovisionamiento están colocados en la unidad CITIC.



Name	Type	Name	Type
User Two	User	Administrator SDDC	User
User Three	User		
User One	User		
Manager Two	User		
Manager One	User		

Figura 4.13: Usuarios dentro de Active Directory

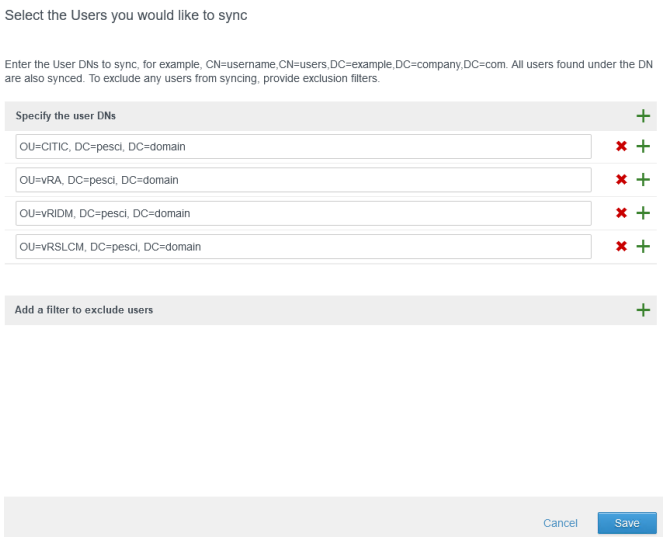
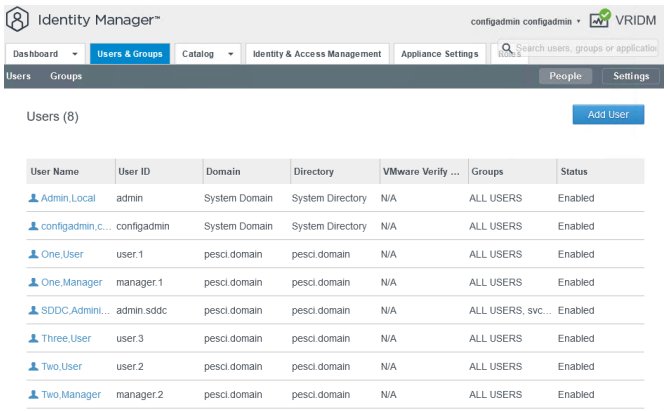


Figura 4.14: Sincronización de usuarios desde Workspace One Access.



User Name	User ID	Domain	Directory	VMware Verify ...	Groups	Status
Admin,Local	admin	System Domain	System Directory	N/A	ALL USERS	Enabled
configadmin,c...	configadmin	System Domain	System Directory	N/A	ALL USERS	Enabled
One,User	user.1	pesci.domain	pesci.domain	N/A	ALL USERS	Enabled
One,Manager	manager.1	pesci.domain	pesci.domain	N/A	ALL USERS	Enabled
SDDC,Admini...	admin.sddc	pesci.domain	pesci.domain	N/A	ALL USERS, svc...	Enabled
Three,User	user.3	pesci.domain	pesci.domain	N/A	ALL USERS	Enabled
Two,User	user.2	pesci.domain	pesci.domain	N/A	ALL USERS	Enabled
Two,Manager	manager.2	pesci.domain	pesci.domain	N/A	ALL USERS	Enabled

Figura 4.15: Usuarios sincronizados en Workspace One Access.

El acceso a las aplicaciones está centralizado a través de una plataforma proporcionada por WSA. Cuando el usuario intenta acceder a vRA este es redirigido a una página web donde introduce sus credenciales, WSA comprueba los datos introducidos y vuelve a redirigir al usuario a la plataforma de vRA. Además, utilizando esta plataforma el administrador puede obtener estadísticas sobre que usuarios se autentican, a que servicios acceden y desde donde lo hacen. WSA permite al administrador editar la interfaz de la web de autenticación, pudiendo personalizar el icono y nombres que se muestran, y modificar los parámetros que se utilizan para autenticarse o mantener las sesiones, permitiendo definir si el usuario debe utilizar su cuenta de correo electrónico o nombre de usuario y si se utilizan cookies de sesión o persistentes. Por si esto fuera poco, también existe la posibilidad de crear políticas para controlar como se autentican los usuarios, desde donde pueden hacerlo y el tiempo de duración de la sesión. En la siguiente figura se muestran las reglas de la política por defecto que se aplica a los usuarios, se permite el acceso desde cualquier dirección IP, a través de un navegador web o la aplicación para dispositivos móviles Workspace One App, usando su contraseña y con un tiempo de sesión de 2160 u 8 horas dependiendo del punto de acceso.

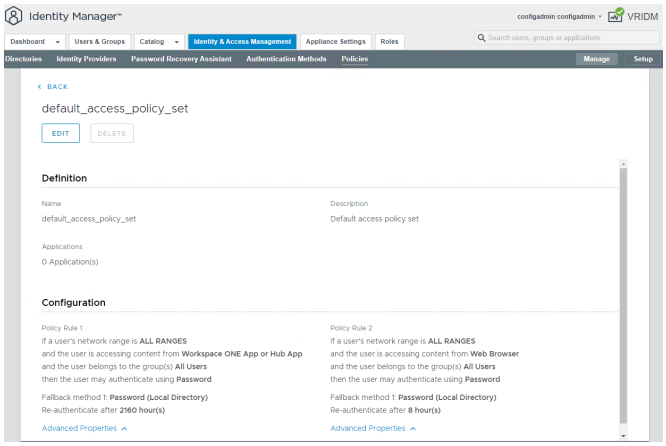


Figura 4.16: Política de autenticación por defecto.

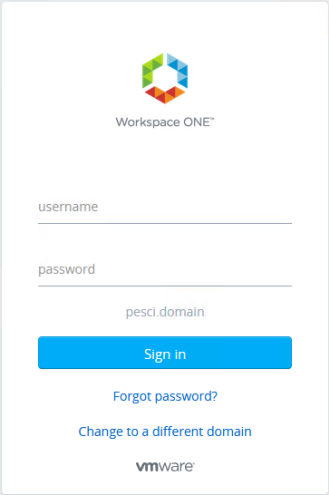


Figura 4.17: Plataforma de autenticación de Workspace One Access

Con WSA el administrador tiene un mayor control sobre los usuarios y como estos acceden a los servicios de la plataforma Cloud, ya que gestiona desde un único punto todas las cuentas de usuarios y la seguridad del punto de acceso, pudiendo controlar que usuarios acceden y estableciendo medidas seguridad de forma sencilla e intuitiva. También, la gestión de las credenciales de cada usuario se separa de la gestión del acceso, ya que lo primero está controlado por Active Directory y lo segundo por WSA. De esta forma, la seguridad del entorno aumenta y las tareas del administrador se simplifican. Con esta plataforma se soluciona uno de los problemas de la infraestructura del CITIC, ya no es necesario crear cuentas manualmente para cada usuario que quiera acceder al servicio y su gestión se hace más dinámica, a la vez que se aumenta el nivel de seguridad.

VMware vRealize Automation

VMware vRealize Automation es el componente de VMware vRealize Suite que automatiza el aprovisionamiento de recursos del SDDC. Con esta plataforma los usuarios podrán elaborar diseños de los recursos que necesitan para posteriormente implementarlos y llevar a cabo sus trabajos. El proceso de implementación es automático y transparente para el usuario que puede modificar los requisitos de sus recursos según sea necesario. Al mismo tiempo, el administrador establece los límites del diseño/implementación y debe proveer en la infraestructura los medios que se usarán como base para los diseños. En vRA el aprovisionamiento de recursos se realiza a partir de diseños realizados por el usuario. Estos diseños, llamados Blueprints, son archivos con formato .yaml en los que se especifican los recursos que el usuario quiere obtener, estos recursos son VMs, redes y almacenamiento, y para cada recurso definido el usuario puede especificar sus características como el tamaño de una VM y su configuración

interna (sistema operativo, instalación de librerías o servicios, redes a las que se conecta). Las blueprints se definen dentro de proyectos en los cuales existen jefes de proyecto y usuarios que utilizan o aprovisionan los recursos definidos en cada blueprint, de esta forma, tanto el administrador como el jefe de proyecto controlan qué usuarios acceden a los recursos de un proyecto. Además, el administrador será el encargado de limitar la cantidad de recursos disponibles para cada proyecto, y de establecer los recursos disponibles para el proyecto, es decir, qué sistemas operativos están disponibles, en qué redes se podrán realizar los despliegues y que datastore utilizarán para el almacenamiento.

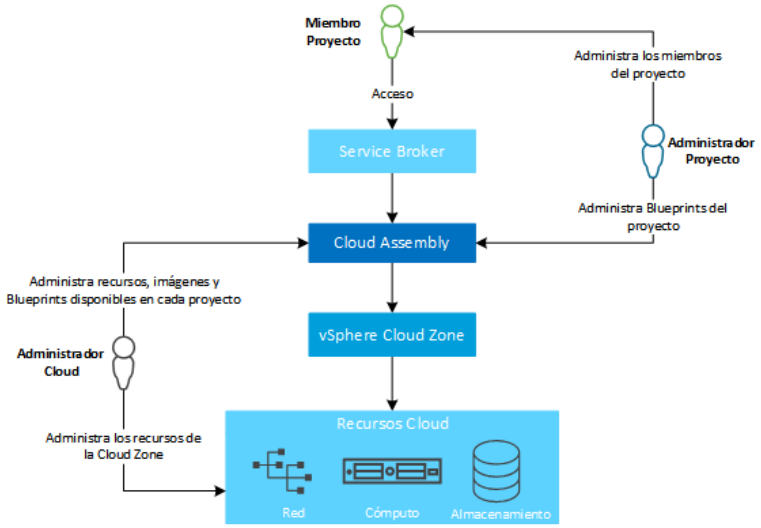


Figura 4.18: Uso y componentes de VMware vRealize Automation.

Como se muestra en la figura anterior, en vRA existen tres componentes principales que son Service Borker, a través del cual los usuarios tienen acceso al catálogo de diseños disponibles en su proyecto para implementarlos, Cloud Assembly, desde donde se elaboran los diseños, automatiza el aprovisionamiento ordenado desde Service Broker y administra la infraestructura disponible, y Cloud Zone, punto desde donde vRA accede a la infraestructura para obtener los recursos, situada en este caso en el cluster vSphere del Management Domain.

Para ordenar el aprovisionamiento de los recursos, antes de realizar cualquier implementación, es necesario configurar la infraestructura que se va a poner a disposición de los usuarios. En VMware vCenter Server, dentro del cluster vSphere se define un *resource pool* y una carpeta que se utilizarán para colocar las VMs que se desplieguen desde vRA. La red que utilizarán las VMs generadas estará controlada por VMware NSX-T para aprovechar las ventajas de sus redes definidas por software y así automatizar su configuración y hacer uso de los servicios que ofrece. Para ello se añade un Segment al router virtual de Tier-1 que se muestra en la figura 4.10, VMware NSX-T informa de la nueva ruta al router físico mediante BGP proporcionando así acceso a redes externas.

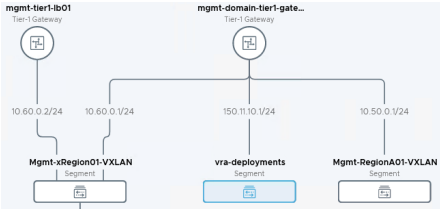


Figura 4.19: Nuevo Segment *vra-deployments* en el router virtual Tier-1.

Las VMs que los usuarios generan están basadas en plantillas que son creadas previamente por el administrador. Antes de generar la plantilla el administrador debe crear una VM en VMware vCenter Server y proveerla con una configuración mínima para que el usuario pueda aplicar su propia configuración durante el despliegue, para este entorno se crea una VM con el sistema operativo Ubuntu Server 20.04.1. Una vez se termina el proceso de instalación y actualización del sistema operativo, se configura el servicio **cloud-init**[12] el cual permite inicializar la VM con la configuración indicada en la blueprint, como se verá más adelante. También se pueden preinstalar servicios como bases de datos para que el usuario solo tenga que configurarlo. Cuando la configuración de la VM está lista, se limpia limpian el hostname, archivos de logs, claves SSH y caché del servicio cloud-init ejecutando el siguiente script, para que en cada implementación se genere una VM distinta a partir de la misma plantilla. Finalmente, la VM se convierte a una plantilla que se almacena en VMware vCenter Server.

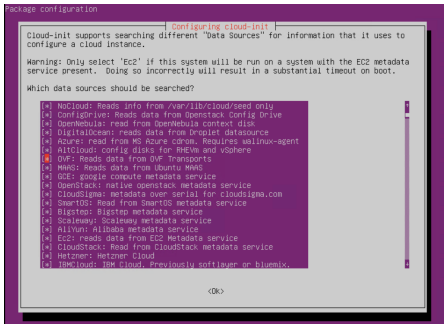


Figura 4.20: Configuración del servicio cloud-init en Ubuntu Server 20.

[12]Se puede encontrar más información sobre cloud-init en el enlace: https://cloudinit.readthedocs.io/en/latest/

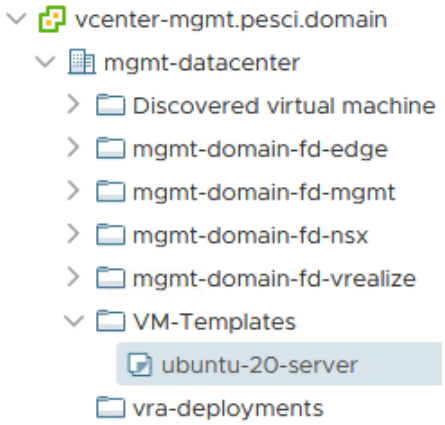


Figura 4.21: Creación de una plantilla a partir de la VM de Ubuntu Server 20.

Apéndices

Apéndice A

Material adicional

Shell script para la limpieza de una máquina virtual Ubuntu después de haber configurado cloud-init. Obtenido del siguiente repositorio https://github.com/jimangel/ubuntu-18.04-scripts.

```
#!/bin/bash
#####################################################
#### WARNING PIPING TO BASH IS STUPID: DO NOT USE THIS
#####################################################
# modified from: jcppkkk/prepare-ubuntu-template.sh
# TESTED ON UBUNTU 18.04 LTS

if [ `id -u` -ne 0 ]; then
  echo Need sudo
  exit 1
fi

set -v

#update apt-cache
apt update -y
apt upgrade -y

#install packages
apt install -y open-vm-tools

#Stop services for cleanup
service rsyslog stop

#clear audit logs
if [ -f /var/log/wtmp ]; then
    truncate -s0 /var/log/wtmp
fi
```

```
if [ -f /var/log/lastlog ]; then
    truncate -s0 /var/log/lastlog
fi

#cleanup /tmp directories
rm -rf /tmp/*
rm -rf /var/tmp/*

#cleanup current ssh keys
rm -f /etc/ssh/ssh_host_*

#add check for ssh keys on reboot...regenerate if neccessary
cat << 'EOL' | sudo tee /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "" on success or any other
# value on error.
#
# In order to enable or disable this script just change the
    execution
# bits.
#
# By default this script does nothing.

# dynamically create hostname (optional)
if hostname | grep localhost; then
    hostnamectl set-hostname "$(head /dev/urandom | tr -dc
    A-Za-z0-9 | head -c 13 ; echo '')"
fi

test -f /etc/ssh/ssh_host_dsa_key || dpkg-reconfigure openssh-server
exit 0
EOL

# make sure the script is executable
chmod +x /etc/rc.local

#reset hostname
# prevent cloudconfig from preserving the original hostname
sed -i 's/preserve_hostname: false/preserve_hostname: true/g'
    /etc/cloud/cloud.cfg
truncate -s0 /etc/hostname
hostnamectl set-hostname localhost
```

```
72
73 #cleanup apt
74 apt clean
75
76 # disable swap
77 sudo swapoff --all
78 sudo sed -ri '/\sswap\s/s/^#?/#/' /etc/fstab
79
80 # set dhcp to use mac - this is a little bit of a hack but I need
    this to be placed under the active nic settings
81 # also look in /etc/netplan for other config files
82 sed -i 's/optional: true/dhcp-identifier: mac/g'
    /etc/netplan/50-cloud-init.yaml
83
84 # cleans out all of the cloud-init cache / logs - this is mainly
    cleaning out networking info
85 sudo cloud-init clean --logs
86
87 #cleanup shell history
88 cat /dev/null > ~/.bash_history && history -c
89 history -w
90
91 #shutdown
92 shutdown -h now
```

Notas

En este documento se utilizan términos en inglés ya que forman parte del campo que se está tratando o por ser su nombre original y por lo tanto están reconocidos.

Cuando en el documento se menciona

capa 2 o

capa 3 se está haciendo referencia a las capas establecidas por el Modelo OSI, la capa de enlace de datos y la capa de red respectivamente.

Lista de acrónimos

API *Application Programming Interface*

AS *Autonomous System*

AZ *Availability Zone*

BGP *Border Gateway Protocol*

BUM *Broadcast, Unknown Unicast, Multiacast*

CA *Certificate Authority*

CITIC *Centro de Invesitgación en Tecnoloxías da Información e as Comunicacións*

CPD *Centro de Procesamiento de Datos*

DHCP *Dynamic Host Configuration ProtocoL*

DNS *Domain Name Server*

DPM *vSphere Distributed Power Management*

DR *Distributed Router*

DRS *vSphere Distributed Resources Scheduler*

FTT *Failures To Tolerate*

HA *vSphere High Availability*

HDD *Hard Disk Drive*

IP *Internet Protocol*

iSCSI *Internet Small Computer System Interface*

LUN *Logical Unit Number*

MD *Management Domain*

MTU *Maximum Transmission Unit*

NAT *Network Address Translation*

NFS *Network File System*

NIST *National Institute of Standards and Technology*

NIC *Network Interface Card*

NTP *Network Time Protocol*

N-VDS *NSX-T Virtual Distributed Switch*

PSC *Platform Services Controller*

QoS *Quality of Service*

RAID *Redundant Array of Independent Disks*

SAN *Storage Area Network*

SDDC *Software Defined Data Center*

SFP *Small Form-factor Pluggable Transceptor*

SMTP *Simple Mail Transfer Protocol*

SSD *Solid-State Drive*

SR *Service Router*

TB *TeraByte*

TEP *Tunnel End Point*

ToR *Switch Top of Rack*

TN *Transport Node*

TZ *Transport Zone*

UDC *Universidade da Coruña*

UDP *User Datagram Protocol*

VCF *VMware Cloud Foundation*

VLAN *Virtual Local Area Network*

VLC *VMware Lab Constructor*

vDS *vSphere Distribute Switch*

VI *Virtual Infrastructure Domain*

VMFS *Virtual Machine File System*

VM *Virtual Machine*

VNI *Virtual Network Identifier*

vRA *VMware vRealize Automation*

vRSLCM *VMware vRealize Lifecycle Manager*

WD *Workload Domain*

WSA *Workspace One Access*

Glosario

Appliance : archivo que contiene una máquina virtual con un sistema operativo con el propósito de entregar una única aplicación preconfigurada.

BGP [8]: protocolo de enrutamiento que se utiliza para el intercambio de rutas entre Autonomous Systems (AS) de forma dinámica y así evitar configurarlas manualmente.

BUM : se refiere al tráfico de red Broadcast, Unknown unicast y Multicast. El primero es tráfico que se transmite a todos los dispositivos disponibles en la red, Unknown Unicast es tráfico enviado a un único destinatario para el que no se conoce su dirección MAC dentro de una misma VLAN y Multicast es tráfico que se envía a los dispositivos que pertenecen a un grupo dentro de una red.

Cluster [9]: agrupación de recursos de múltiples hosts que se gestionan como una única colección.

Controlador SFP+ : interfaz modular que permite conectar cables de fibra óptica a un dispositivo.

CPD : luegar donde se sitúan un conjunto recursos con gran capacidad de cómputo necesarios para procesar información, normalmente en grandes cantidades.

Datastore : dentro de VMware vSphere, un datastore es un contenedor lógico que abstrae los componentes físicos de almacenamiento y provee un modelo uniforme para almacenar máquinas virtuales, plantillas o imágenes ISO.

Hipervisor baremetal : software instalado sobre el hardware de un servidor que permite instalar aplicaciones que funcionan sobre entornos virtuales directamente sobre el hardware.

Host : servidor físico en el que se ejecuta el hipervisor.

IaaS [2]: servicio Cloud en el que se provee capacidad de aprovisionamiento de recursos de cómputo, almacenamiento y red, sobre los cuales se puede desplegar software.

iSCSI : estándar que implementa el protocolo de transporte SCSI para transmitir datos entre dispositivos.

Jumbo Frame [10]: paquetes de red cuyo MTU es mayor que el valor definido en el estándar Ethernet, 1500.

LUN : identifica una colección de dispositivos de almacenamiento que se presentan como un único volumen.

Máquina virtual : máquina que se ejecuta en un entorno virtualizado con hardware virtual detro de un hipervisor.

NIC : componente físico que conecta un dispositivo a una red y permite compartir sus recursos.

Pool de almacenamiento : agrupación de volúmenes de almacenamiento que se administran de forma conjunta.

Port Group : puertos que se añaden en el componente vSphere Distributed Switch y que agrupan las conexiones de múltiples máquinas virtuales sobre las cuales se pueden establecer una configuración determinada.

QoS : medida de rendimiento que se asigna a un servicio en la red. Los componentes de VMware utilizan el campo Differentiated Services Code Point (DSCP) en la cabecera de capa 3, y el campo Class of Service (CoS) en la cabecera de capa 2 para indicar la prioridad del tráfico.

Rack : armario metálico destinado a alojar servidores físicos.

RAID 5 : conjunto de discos duros que funciona como una única unidad de almacenamiento para aumentar el rendimiento y la eficiencia. RAID 5 necesita como mínimo tres discos duros, y distribuye de paridad en todos los discos para poder recuperar datos corruptos.

Red Overlay [11]: abstracción de una red sobre una red física implementada por un conjunto de nodos situados en diferentes localizaciones y conectados entre si.

SAN : red dedicada a proveer acceso a los dispositivos de almacenamiento.

SDDC [12]: Software-Defined Datacenter es un modelo de arquitectura de infraestructura para virtualizar los recursos de cómputo, almacenamiento y red.

UDP : protocolo de red de la capa de transporte que permite enviar paquetes sin establecer previamente una conexión.

VLAN : método para aislar múltiples dominios de broadcast sobre una misma red física.

VLAN trunk : enlace que permite la circulación del tráfico de diferentes redes VLAN.

Bibliografía

[1] "Vmware vsphere entreprise edition datasheet." [Online]. Available: https://www.vmware.com/files/es/pdf/VMware-vSphere-Entreprise-Edition-Datasheet.pdf

[2] T. G. Peter Mell, "The NIST Definition of Cloud Computing." [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[3] CITC, "Centro de Procesado de Datos." [En línea]. Disponible en: https://www.citic.udc.es/instalacion/centro-de-despliegue.html

[4] VmWare, "Cloud foundation components." [En línea]. Disponible en: https://docs.vmware.com/en/VMware-Cloud-Foundation/4.0/rn/VMware-Cloud-Foundation-40-Release-Notes.html#swversions

[5] V. vSAN, "vsan disk groups and data storage architecture: Hybrid or all-flash." [En línea]. Disponible en: https://youtu.be/PDcLgV37FP4?list=PLjwkgfjHppDux1XhPB8pW3vS43Aglfq2c

[6] V. C. Foundation, "Vmware software licenses." [En línea]. Disponible en: https://docs.vmware.com/en/VMware-Cloud-Foundation/3.9/com.vmware.vcf.planprep.doc_39/GUID-202ECBCF-2CAA-4167-BA54-4EE1169D312C.html

[7] VMware, "vsan all flash hardware guidance (af-4 series)," 2020. [En línea]. Disponible en: https://www.vmware.com/resources/compatibility/vsan_profile.html?locale=en

[8] P. Traina, "Bgp-4 protocol analysis," RFC 1774, DDN Network Information Center, Tech. Rep., 1995.

[9] V. Infrastructure, "Resource management with vmware drs," *VMware Whitepaper*, vol. 13, 2006.

[10] E. Alliance and B. Kohl, "Ethernet jumbo frames," 2009.

[11] D. Gifford, K. L. Johnson, M. F. Kaashoek, and J. W. O'Toole Jr, "Overcast: Reliable multicasting with an overlay network," in *Proceedings of USENIX Symposium on OSDI*, 2000.

[12] V. Törhönen, "Designing a software-defined datacenter," 2013. [En línea]. Disponible en: http://urn.fi/URN:NBN:fi:tty-201405261235