



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

# PESCI: Plataforma de Entrega de Servicios Cloud para Investigación

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

A Coruña, novembro 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. 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 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

---

<b>1</b>	<b>Introducción</b>	<b>1</b>
1.1	Motivación . . . . .	2
1.2	Objetivos . . . . .	3
1.3	Organización . . . . .	3
<b>2</b>	<b>Estado de los recursos</b>	<b>5</b>
2.1	Infraestructura . . . . .	5
2.1.1	Cómputo . . . . .	5
2.1.2	Almacenamiento . . . . .	5
2.1.3	Red . . . . .	6
2.2	Software . . . . .	6
<b>3</b>	<b>Planificación</b>	<b>9</b>
3.1	Tareas y costes del proyecto . . . . .	9
<b>4</b>	<b>Estado de la tecnología</b>	<b>13</b>
4.1	Servicio Cloud . . . . .	13
4.1.1	VMware Cloud Foundation . . . . .	14
4.1.2	Componentes de VMware Cloud Foundation . . . . .	15
4.1.3	Conceptos . . . . .	18
4.1.4	Costes de implementación . . . . .	22
<b>5</b>	<b>Metodología</b>	<b>25</b>
5.1	Requisitos . . . . .	25
5.1.1	Cómputo . . . . .	25
5.1.2	Almacenamiento . . . . .	26
5.1.3	Red . . . . .	26
5.2	Prueba de concepto . . . . .	27

5.2.1	Preparación . . . . .	27
5.2.2	Diseño y configuración del Management Domain . . . . .	29
5.2.3	Operaciones de la Arquitectura . . . . .	37
5.2.4	Servicio Cloud . . . . .	44
<b>A</b>	<b>Material adicional</b>	<b>65</b>
A.1	Diseño WD-Server para vRealize Automation . . . . .	65
A.2	Diseño Wordpress-MySQL-Embedded para vRealize Automation . . . . .	67
<b>Notas</b>		<b>71</b>
<b>Lista de acrónimos</b>		<b>73</b>
<b>Glosario</b>		<b>75</b>
<b>Bibliografía</b>		<b>77</b>

# Índice de figuras

---

2.1 Componentes de VMware vSphere[1] . . . . .	7
2.2 Componentes físicos y software que forman la infraestructura actual del CITIC. . . . .	8
3.1 Estadísticas sobre la planificación del proyecto. . . . .	11
3.2 Diagrama de Grantt sobre la planificación del proyecto. . . . .	12
4.1 Estructura de VMare Cloud Foundation. . . . .	15
4.2 Elementos de un SDDC gestionado con VMware Cloud Foundation. . . . .	15
4.3 Partes de un SDDC y componentes de VCF que las implementan. . . . .	16
4.4 Configuración <i>All-Flash</i> y configuración <i>Hybrid</i> en vSAN. . . . .	17
4.5 Componentes de VMware NSX-T y capas en las que se dividen. . . . .	17
4.6 Esquema del modelo de arquitectura estándar. . . . .	19
4.7 Esquema del modelo de arquitectura consolidado. . . . .	20
4.8 Ejemplo de un SDDC con dos Regions y una AZ en cada uno. . . . .	21
5.1 Herramienta VMware Lab Constructor v4.0.1b . . . . .	28
5.2 Finalización del despliegue inicial de VMware Cloud Foundation. . . . .	29
5.3 Servicios desplegados y entorno embebido generado por VLC dentro del host físico. . . . .	29
5.4 Dominio de la instancia de VMware vCenter Server. . . . .	30
5.5 Contenido de vSphere Distributed Switch <i>sddc-vds01</i> . . . . .	32
5.6 Ejemplo de como se almacena un archivo con VMware vSAN y FTT igual a uno	33
5.7 Segments a los que se conecta cada host del entorno y cómo estos acceden a la red física a través de las VMs de NSX-T Edge. . . . .	35
5.8 Topología virtual de las redes virtuales construidas en VMware NSX-T. . . . .	36
5.9 Componentes con los que se comunica vRSLCM. . . . .	38
5.10 Apartado donde se muestra la configuración de la instancia de WSA en vRSLCM.	39

5.11 Unidades organizativas configuradas en el AD junto a los usuarios pertenecientes a la unidad CITIC. . . . .	40
5.12 Sincronización de usuarios desde Workspace One Access seleccionando Unidades Organizativas. . . . .	40
5.13 Usuarios sincronizados en Workspace One Access. . . . .	41
5.14 Política de autenticación por defecto establecida en WSA. . . . .	42
5.15 Plataforma de autenticación de Workspace One Access. . . . .	42
5.16 Uso y componentes de VMware vRealize Automation. . . . .	43
5.17 Resource pool (izquierda) y carpeta (derecha) creadas para alojar las VMs desplegadas desde vRA. . . . .	44
5.18 Segment utilizado para el despliegue de VMs con vRA (arriba) y la configuración del servidor DHCP definida en VMware NSX-T (abajo) . . . . .	45
5.19 Instalación y preparación de la VM con Windows Server 2016 para la creación de una plantilla . . . . .	46
5.20 Instalación CentOS y comandos ejecutados para la creación de una plantilla. . . . .	46
5.21 Plantillas de CentOS 8 y Windows Server 2016 creadas a partir de sus respectivas VMs. . . . .	47
5.22 Plantillas de CentOS 8 y Windows Server 2016 disponibles en vRA. . . . .	47
5.23 Subred habilitada en vRA que se corresponde con el Segment <i>Mgmt-Region01A-VXLAN</i> configurado en VMware NSX-T. . . . .	48
5.24 Cloud Zone (izquierda) y resource pool (derecha) configurados para utilizar los recursos de cómputo y colocar las VMs desplegadas. . . . .	48
5.25 Perfil de almacenamiento configurado donde se indica el datastore utilizado para aprovisionar recursos de almacenamiento. . . . .	49
5.26 Perfiles donde se preestablecen la cantidad de recursos que puede tomar una VM. . . . .	49
5.27 Tarjeta de cobro para valorar los recursos consumidos por los usuarios. . . . .	50
5.28 Proyectos creados para dar acceso a los usuarios a vRA. . . . .	51
5.29 Usuarios del proyecto Server-Desktop (izquierda) y usuarios del proyecto Web-DB (derecha). . . . .	51
5.30 Diseño WD-Server para el proyecto Server-Desktop. . . . .	52
5.31 Publicación en el catálogo de una nueva versión del diseño. . . . .	53
5.32 Diseño Wordpress-MySQL-Embedded para el proyecto Web-WD. . . . .	53
5.33 Inicio de sesión del usuario <i>User Three</i> (izquierda) y catálogo de diseños disponibles en el proyecto Server-Desktop (derecha). . . . .	54
5.34 Formulario para configurar el nuevo despliegue iniciado por el usuario <i>User Three</i> . . . . .	55

## ÍNDICE DE FIGURAS

---

5.35 Tarjeta del despliegue iniciado por el usuario <i>User Three</i> (arriba) y la monitorización de todas las tareas llevadas a cabo por vRA durante el despliegue (abajo). . . . .	55
5.36 Panel de control de la VM CentOS creada por <i>User Three</i> (izquierda) y panel de control de la VM Windows creada por <i>User Three</i> (derecha). . . . .	56
5.37 Acciones que <i>User Three</i> puede ejecutar sobre las VMs creadas. . . . .	56
5.38 Conexión de <i>User Three</i> mediante RDP a la VM con Windows Server 2016 (arriba) y mediante SSH a la VM con CentOS (abajo). . . . .	57
5.39 Diseños disponibles para <i>User Two</i> (izquierda). Formulario de configuración de un nuevo despliegue del diseño Wordpress-MySQL-Embedded (derecha). .	58
5.40 Despliegues user2-wordpress-blog iniciado por <i>User Two</i> . . . . .	58
5.41 Fragmento de la ejecución de cloud-init donde se instala el paquete php-json y se descargan los archivos para la instalación de Wordpress. . . . .	59
5.42 Panel de control del despliegue iniciado por <i>User Two</i> una vez finalizado. . . .	59
5.43 Página de instalación de Wordpress cuando <i>User Three</i> accede por primera vez (izquierda). Primer artículo escrito por <i>User Two</i> en su nuevo sitio web. . . .	60
5.44 Panel de control del despliegue User2-Wordpress-Blog con la vista de monitorización de la VM Web-DB-CentOS-test-303. . . . .	60



# 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, 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 proponer un servicio Cloud que solucione las carencias del servicio actual del CITIC para proporcionar recursos de forma sencilla y ágil a aquellos usuarios que necesiten equipos de grandes prestaciones. La solución propuesta también servirá para mejorar la gestión interna del servicio reduciendo así 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, con el que 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](#) donde se describe el hardware y el software que forman la infraestructura situada en el CITIC y las carencias que hacen necesario implementar una nueva solución. En el capítulo [3.Planificación](#) se describen las tareas y los costes de la realización de este proyecto. Posteriormente, en el capítulo [4.Estado de la tecnología](#) se describe la situación actual de la tecnología que se quiere implementar, las soluciones encontradas en el mercado que se podrían implementar sobre la infraestructura del CITIC, la descripción y componentes de la solución elegida y los costes de implementarla. Una vez expuestas las bases del proyecto, en el capítulo [5.Metodología](#) se exponen los requisitos físicos y servicios que la infraestructura debe proveer antes de realizar la implementación. Dentro del mismo capítulo en el apartado [5.2.Prueba de concepto](#), se exponen la instalación y funcionalidades de los componentes de la solución propuesta dentro de un entorno de pruebas, y finalmente, en el apartado [5.2.4.Servicio Cloud](#) se describen los casos de uso del servicio construido y cómo sería el flujo de trabajo de los usuarios y el administrador de la infraestructura.

---

*1.3. Organización*

## 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 gran rendimiento de cómputo y flexibilidad en cuanto a que permiten escalar la infraestructura.

### 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 aportar 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 de las conexiones entre hosts, cada host se conecta a dos switches *trunk* estableciendo rutas redundantes. En caso de que fuera necesario modificar la estructura de la red para adaptarse a los requisitos de un determinado despliegue, habría que hacerlo directamente sobre la red física. Esto puede generar problemas en la conectividad del entorno a parte de tener un 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 parte de 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.

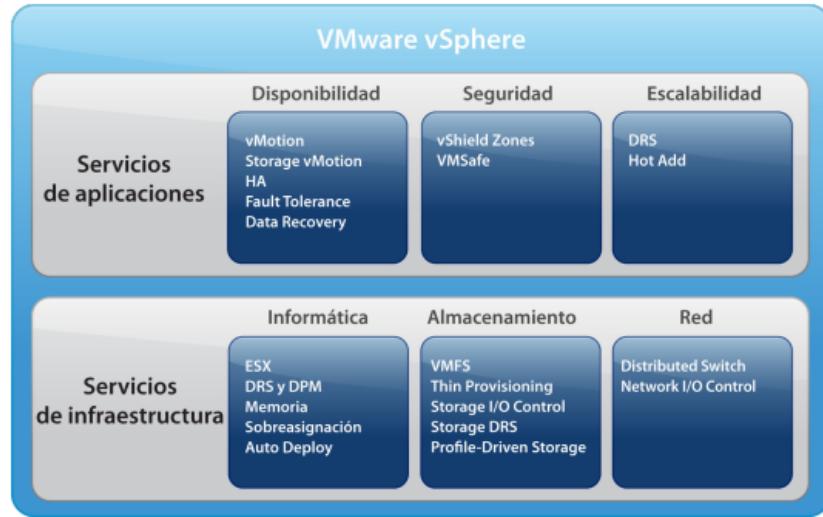


Figura 2.1: Componentes de VMware vSphere[1]

En cada host está instalado el hipervisor ESXi de tipo baremetal, el cual se encarga de habilitar la virtualización de los recursos. Sobre los hosts se encuentra 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 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. 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: encargado 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.

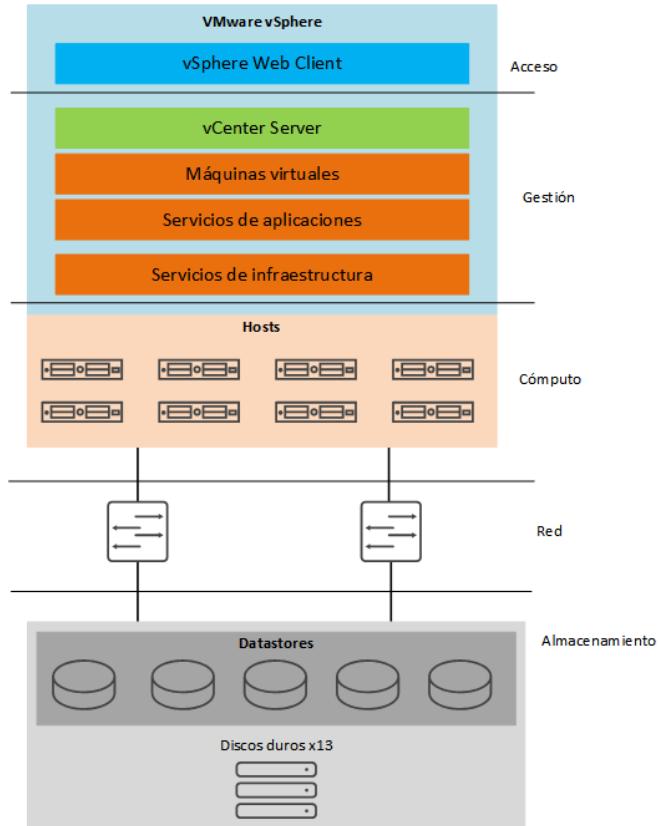


Figura 2.2: Componentes físicos y software que forman la infraestructura actual del CITIC.

## Capítulo 3

# Planificación

---

**E**n 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 y costes del proyecto

Tarea 1. Analizar qué componentes hardware y software componen la infraestructura y cuales son sus funciones. En cuanto al hardware se comprueban las especificaciones concretas de los recursos de cómputo, almacenamiento y red, y cómo están estructurados el sistema de almacenamiento y la red. Respecto al software se comprueba qué productos y servicios hay instalados y cuales son sus funciones dentro del entorno.

Tarea 2. Analizar y seleccionar una herramienta de las disponibles en el mercado que se adapte a los objetivos del servicio que se quiere construir y a las características de la infraestructura. En este proceso se tiene en cuenta la compatibilidad con el software ya existente, el coste de mantenimiento y la eficiencia de las herramientas disponibles.

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

Tareas 4, 5, 6, 7, 8, 9 y 10. Antes de realizar la instalación de la nueva herramienta es necesario comprobar sus requisitos software y hardware (tareas 4 y 5). También se deben establecer los parámetros de configuración iniciales que se van a aplicar a la nueva plataforma (tarea 6). Construcción de un entorno de pruebas con una infraestructura que se adapte a los requisitos de la herramienta seleccionada y así evitar problemas en el entorno real del CITIC (tareas 7 y 8). Una vez el entorno está preparado se efectúa el despliegue de la herramienta(tarea 9), posteriormente se configura y se comprueba el funcionamiento del nuevo servicio (tarea 10).

Tarea 11. Esta tarea marca el final del despliegue y configuración del nuevo servicio en la in-

fraestructura.

Tarea 12. Diseñar una integración de la nueva plataforma con el sistema de autenticación de la UDC para que los usuarios finales del servicio puedan autenticarse sin necesitar nuevas credenciales. Se debe utilizar un directorio de usuarios que simule el directorio de la UDC y así evitar problemas en el entorno de producción.

Tarea 13. Implementación y despliegue de la solución que permita integrar el directorio de usuarios del entorno de pruebas con la herramienta desplegada para la autenticación de usuarios con sus propias credenciales.

Tarea 14. Diseño de un sistema de facturación/valoración del consumo de recursos por parte de los usuarios con la intención de limitar la cantidad de recursos que un usuario puede aprovisionar, y así tener recursos disponibles para todos los usuarios y aumentar la eficiencia la eficiencia de la infraestructura.

Tarea 15. Implementación y despliegue del sistema de facturación/valoración.

Tarea 16, 17 y 18. 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 se realiza.

Tarea 19, 20 y 21. 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 su realización y proponer una solución para habilitar un servicio Cloud en la infraestructura del CITIC. La escritura de este documento se realiza a la vez que 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 en la figura 3.1 se refiere al coste correspondiente al estudiante si trabaja por 25 €/hora.

### CAPÍTULO 3. PLANIFICACIÓN

---

	Comienzo	Fin	
Actual	mar 04/02/20	vie 17/04/20	
Previsto	mar 04/02/20	mar 14/04/20	
Real	NOD	NOD	
Variación	0d	6d	
	Duración	Trabajo	Costo
Actual	106,75d	207,25h	5.181,25 €
Previsto	100,75d	201,25h	5.031,25 €
Real	0d	0h	0,00 €
Restante	106,75d	207,25h	5.181,25 €

Figura 3.1: Estadísticas sobre la planificación del proyecto.

### 3.1. Tareas y costes del proyecto

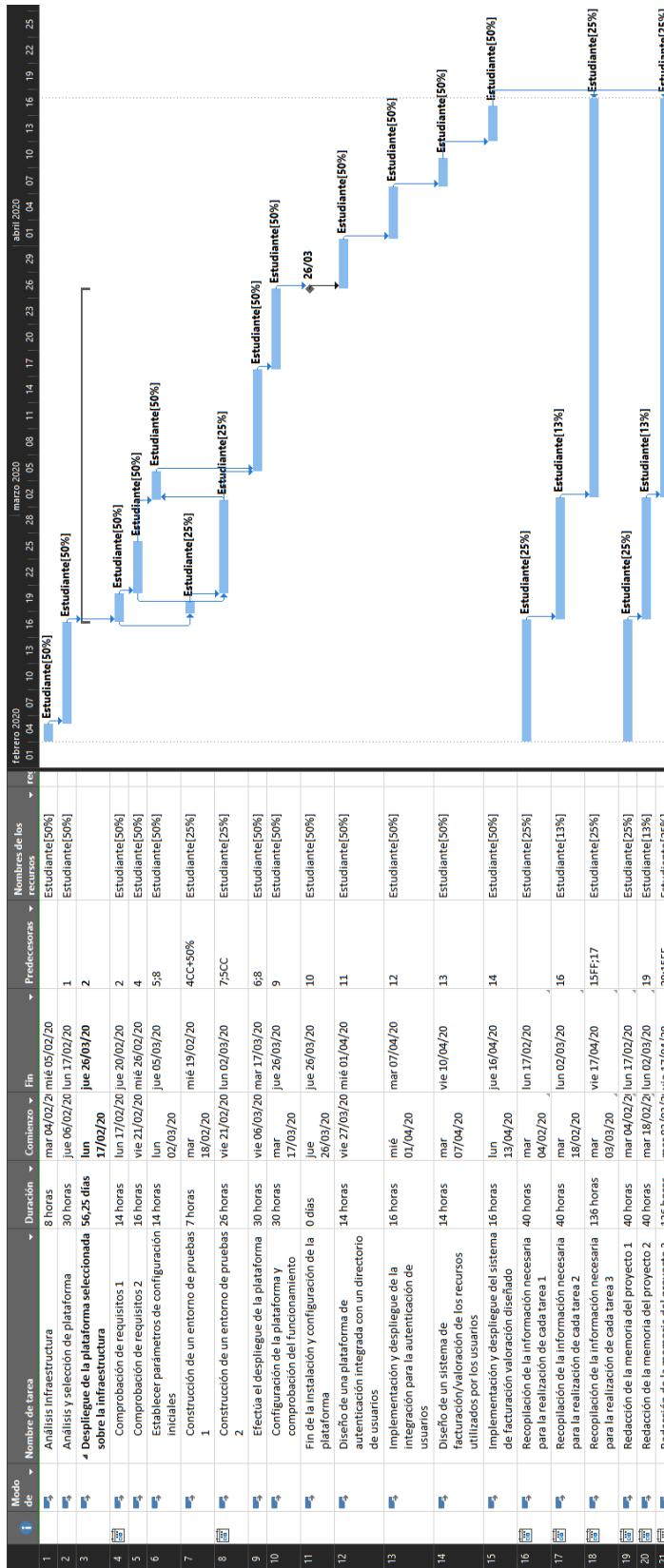


Figura 3.2: Diagrama de Gantt sobre la planificación del proyecto.

## Capítulo 4

# 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 para 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. A lo largo de este capítulo se expone la solución Cloud propuesta para ser implementada en la infraestructura del CITIC indicando las razones de su elección y sus principales características.

### 4.1 Servicio Cloud

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 al pertenecer al mismo proveedor que el software de virtualización empleado en la infraestructura del CITIC, todos sus componentes se integran perfectamente con los componentes de VMware ya instalados en la infraestructura, por lo tanto, su mantenimiento es más sencillo y su funcionamiento más eficiente. También es posible integrar soluciones de otras compañías pero, al estar fuera del ecosistema de VMware podrían producirse problemas de compatibilidad entre versiones a largo plazo con los productos existentes en la infraestructura del CITIC. Utilizando los productos de un mismo proveedor se asegura el soporte del software instalado y la obtención del máximo rendimiento de cada componente.

#### 4.1.1 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 abstraída en una capa virtual separando así la gestión de ambas. Esto permite modificar la infraestructura virtual según se requiera sin necesidad de modificar la configuración de la infraestructura física, favoreciendo la automatización y dinamismo de tareas y la elasticidad de los recursos. Gracias a esto, con VCF es posible habilitar el aprovisionamiento de recursos por parte de los usuarios para ofrecer así un servicio de IaaS. Con esta solución 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.

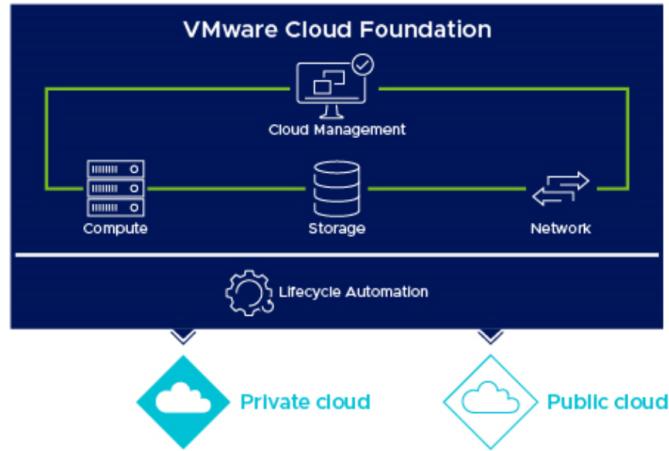


Figura 4.1: Estructura de VMare Cloud Foundation.

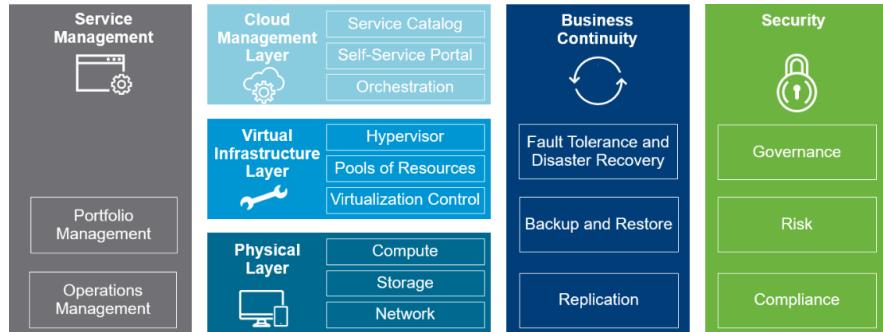


Figura 4.2: Elementos de un SDDC gestionado con VMware Cloud Foundation.

#### 4.1.2 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<sup>1</sup>. 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 8.2 de VMware vRealize Suite.

---

<sup>1</sup>Las características del componente VMware vSphere son las mismas que las descritas en el punto 2.2

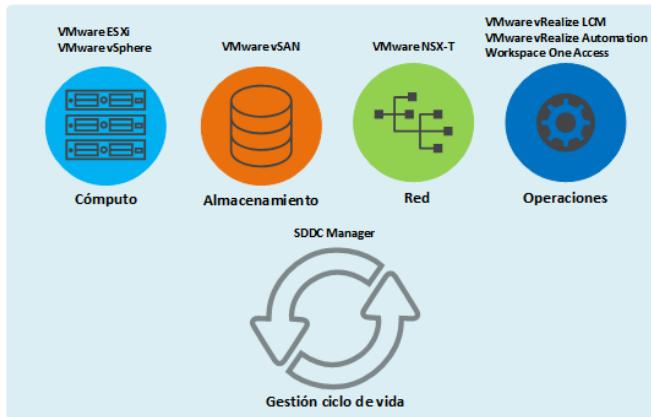


Figura 4.3: Partes de un SDDC y componentes de VCF que las implementan.

### 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.

### VMware vSAN

VMware vSAN virtualiza el almacenamiento del SDDC. Permite gestionar de forma centralizada, 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 mediante el protocolo IP, a través de una subred dedicada al servicio. 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 SSD, 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<sup>[5]</sup>.

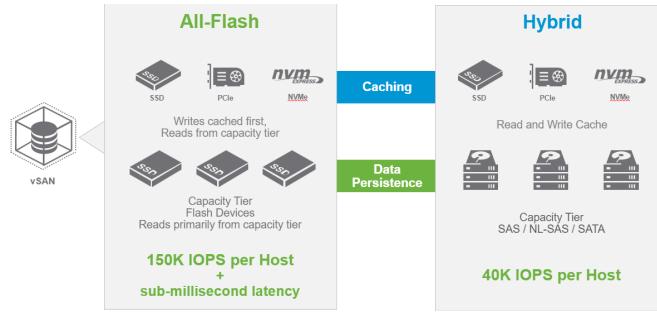


Figura 4.4: Configuración *All-Flash* y configuración *Hybrid* en vSAN.

### VMware NSX-T

VMware NSX-T virtualiza la red del SDDC. Abstactra 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 integrados en VMware NSX-T se encargan de controlar el tráfico y monitorizar la infraestructura virtual creada por VMware NSX-T.

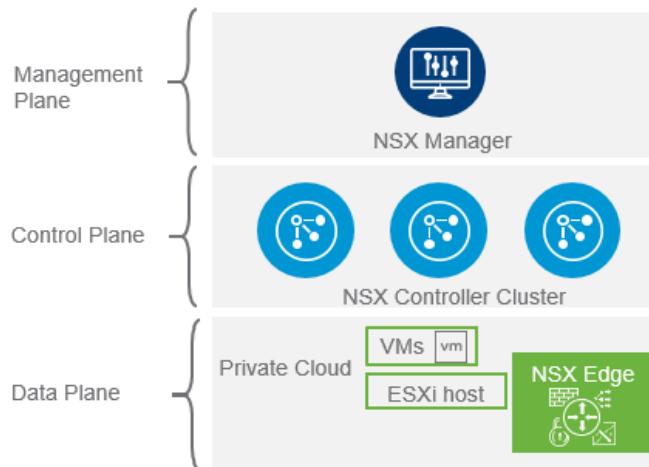


Figura 4.5: Componentes de VMware NSX-T y capas en las que se dividen.

## 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. 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.

### 4.1.3 Conceptos

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

#### Workload Domain

Un Workload Domain (WD) representa un bloque de recursos dentro del SDDC, formado por recursos físicos y virtuales y 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, 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 por lo tanto todas las tareas de administración de la infraestructura están centralizadas dentro de este WD. 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.
- Dos VMs de VMware NSX-T Edge.

### 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 objetivo es separar las tareas y recursos dedicados a la administración del SDDC de las tareas y recursos utilizados por los usuarios del servicio. 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 situadas en el Management Domain.
- Dos VMs de VMware NSX-T Edge.

### Modelo de arquitectura 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.

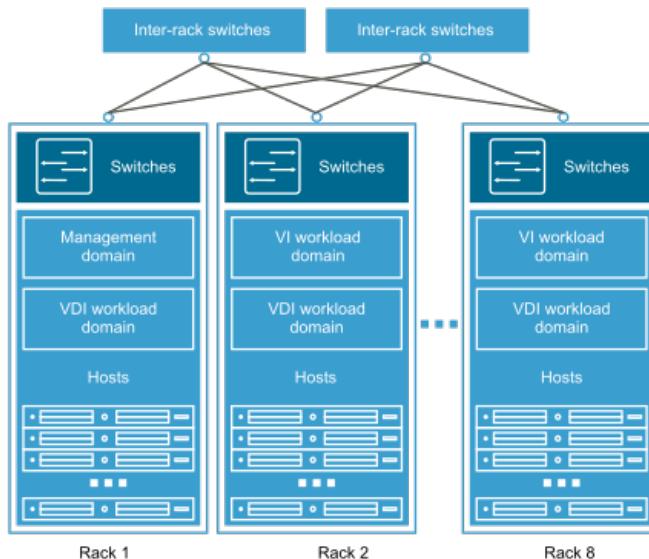


Figura 4.6: Esquema del modelo de arquitectura estándar.

### Modelo de arquitectura 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<sup>2</sup> 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 grupos, llamados 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 realizan sobre los mismos recursos, y los niveles de control y seguridad son menores.

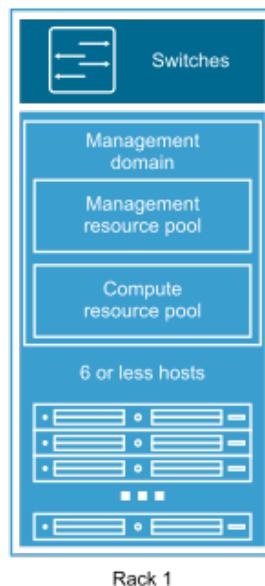


Figura 4.7: Esquema del modelo de arquitectura consolidado.

### Distribución de los recursos del SDDC

Los recursos de un SDDC pueden estar distribuidos en diferentes localizaciones físicas para proporcionar mayor disponibilidad y recuperación ante fallos. A continuación se enumeran las formas de agrupar los recursos según su ubicación.

- 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

---

<sup>2</sup>Se despliega la misma cantidad de instancias de cada componente que en el Management Domain.

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 minimizando 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[6] 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[6]. 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 VMs desplegadas sobre ellos se les aplica una configuración de disponibilidad con los servicios vMotion, vSphere HA y vSphere DRS del 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.

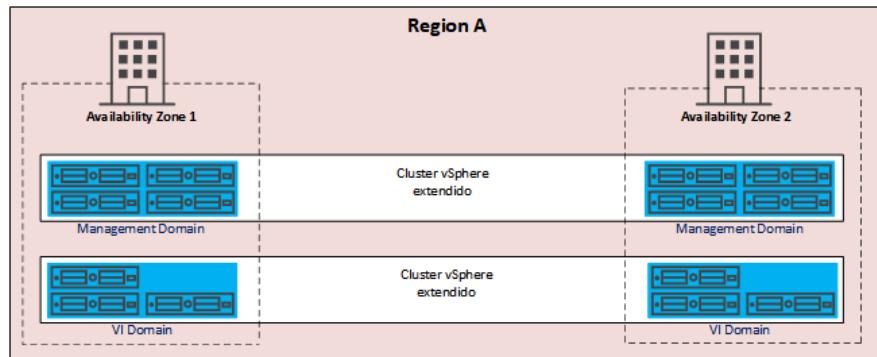


Figura 4.8: Ejemplo de un SDDC con dos Regions y una AZ en cada uno.

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 VMs 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 reali-

zan 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<sup>3</sup>.

#### 4.1.4 Costes de implementación

Los principales costes a la hora de implementar VMware Cloud Foundation en la infraestructura de producción del CITIC son aquellos relacionados con la adquisición de licencias y soporte de los productos. Cada componente de VMware Cloud Foundation requiere su propia licencia[7]. El precio de cada licencia dependerá del número de CPUs físicas sobre las que se va usar esta plataforma. 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€<sup>4</sup> 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€<sup>5</sup> 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€<sup>6</sup> 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€<sup>7</sup> 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 NSX-T:** 5.300€<sup>8</sup> 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 Suite 2019:** 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

<sup>3</sup>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>

<sup>4</sup>Para la edición *Advanced* de VMware Cloud Foundation.

<sup>5</sup>Para la edición *Standard* de VMware vSphere.

<sup>6</sup>Para la edición *Standard* de VMware vCenter

<sup>7</sup>Para la edición *Advanced* de VMware vSAN.

<sup>8</sup>Para la edición *Advanced* de NSX.

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-T y VMware vRealize Suite 2019. El coste total de la instalación y mantenimiento de la plataforma VMware Cloud Foundation sobre la infraestructura del CITIC es el siguiente:

- **Licencias:** 460.400€ en total.
- **Soporte:** 164.600€ anuales.



## Capítulo 5

# Metodología

---

**E**n este capítulo se describirá el desarrollo del proyecto y las funcionalidades más destacadas de la solución implementada. Para ello se describirán los requisitos para implementar VCF en un entorno real, el proceso de despliegue del producto sobre un entorno de pruebas junto con sus características y finalmente se demostrará el uso que los usuarios pueden hacer de la solución.

## 5.1 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 sencilla a la hora de expandir el entorno.

### 5.1.1 Cómputo

#### Hosts ESXi

Para realizar el despliegue del primer WD (el Management Domain) se requieren al menos cuatro hosts ESXi con al menos 128 GB de memoria RAM y un disco de arranque de 32 GB cada uno<sup>1</sup>. Para cada WD adicional solo se requiere un mínimo de tres hosts cuya cantidad de memoria RAM depende de la finalidad del WD. Cada uno de los hosts debe tener al menos dos interfaces de red físicas (NIC) que soporten al menos 10 Gbit/seg de velocidad.

---

<sup>1</sup>Según la configuración establecida para el producto vSAN ReadyNode [8]

### 5.1.2 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<sup>2</sup>. Se debe aplicar la configuración All-Flash con discos SSD. Basándose en los perfiles que VMware establece para su producto vSAN Ready Node[8], 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 WDs 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.

### 5.1.3 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. 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.

---

<sup>2</sup>VMware vSAN requiere un mínimo de tres hosts mientras que el Management Domain requiere un mínimo de cuatro hosts.

- 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 para el envío de alertas y comunicación de los usuarios con el administrador del SDDC.
- 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.

## 5.2 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 formado por un host y un datastore, 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 realiza el despliegue de uno o varios componentes y posteriormente se revisa su configuración y funcionamiento. Primero se instalarán los componentes base de VMware Cloud Foundation<sup>3</sup> usando el programa VMware Lab Constructor (VLC) v4.0.1<sup>4</sup>. Despues 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 de recursos. Finalmente, se comprobará el funcionamiento general del SDDC y las posibilidades que ofrece el servicio Cloud desplegado.

### 5.2.1 Preparación

En esta sección se describe como se prepara el entorno de pruebas con los elementos y servicios utilizados para realizar el despliegue de la solución y 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, la cual permite crear un entorno embebido dentro del host utilizado

---

<sup>3</sup>Los componentes base de VCF son VMware vSphere, VMware vSAN y VMware NSX-T

<sup>4</sup>Herramienta que permite crear de forma automatizada un entorno embebido para probar las funcionalidades de VMware Cloud Foundation.

como entorno de pruebas. 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.

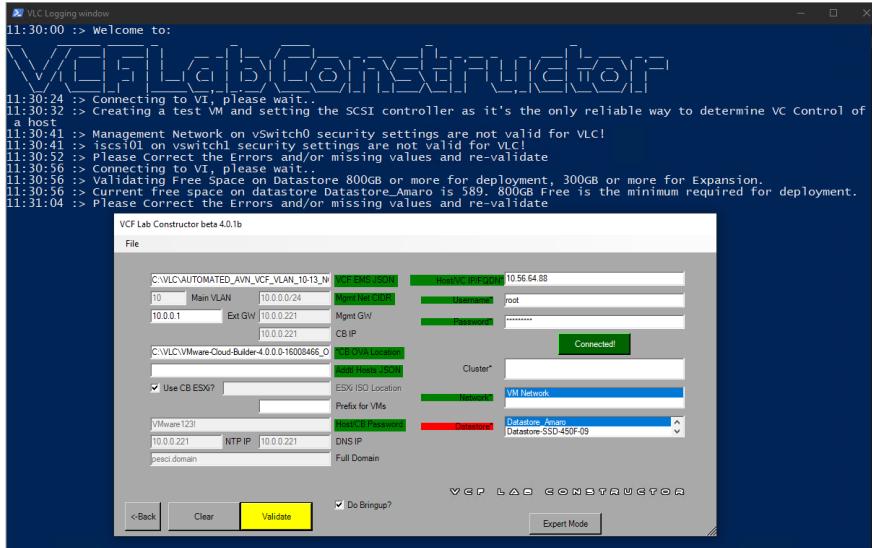


Figura 5.1: Herramienta VMware Lab Constructor v4.0.1b

## 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 3 TB. Además, incorpora dos interfaces de red. La primera interfaz se conecta a una red para acceder al datastore, mientras que la segunda, representada con el nombre *vmnic0* en la figura 5.3, 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 además cuenta con servicio DHCP. El servidor DNS utiliza *pesci.domain* como nombre de dominio. El almacén Active Directory sustituye al directorio de usuarios de la UDC para poder manejar cuentas de usuarios sin causar conflictos en el funcionamiento de los servicios en producción.

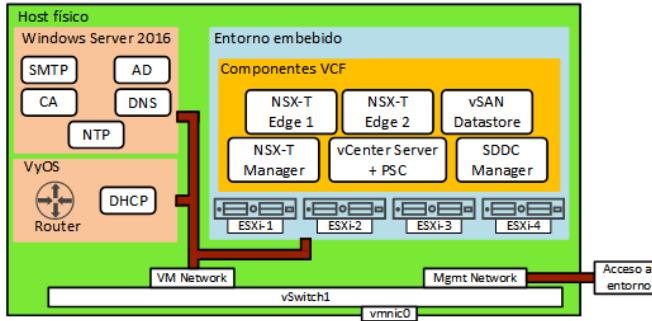


Figura 5.2: Finalización del despliegue inicial de VMware Cloud Foundation.

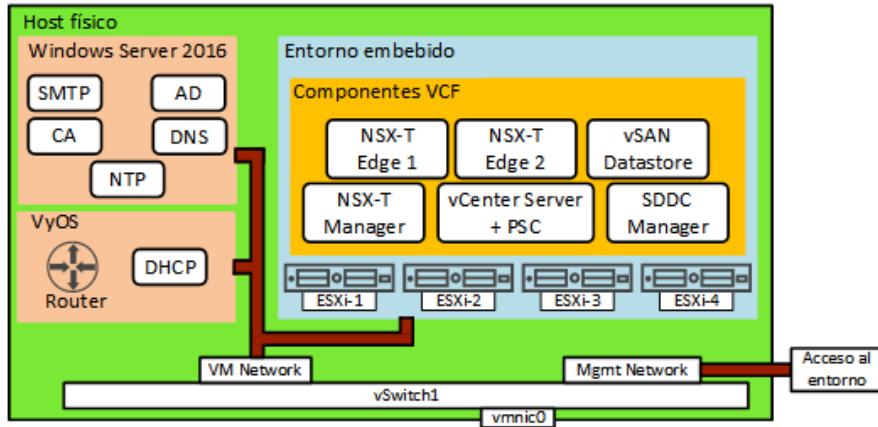


Figura 5.3: Servicios desplegados y entorno embebido generado por VLC dentro del host físico.

Una vez finalizado el despliegue como se muestra en la figura 5.2, el entorno embebido generado con VLC dentro del host físico, incluyendo las VMs de los componentes de VCF y los servicios necesarios para su correcto funcionamiento, se muestra en la figura 5.3. Esta figura también incluye 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.

### 5.2.2 Diseño y configuración del Management Domain

En esta sección se describen las funciones y configuración establecida de los componentes de VCF, tanto los desplegados con la herramienta VLC como los instalados manualmente para completar las funcionalidades de la solución.

## 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. Esta instancia de vCenter Server contiene un dominio con un cluster vSphere que agrupa a los cuatro hosts ESXi que forman el Management Domain. Estos hosts se denominan respectivamente *esxi-1*, *esxi-2*, *esxi-3* y *esxi-4*, el primero cuenta con 96 GB de memoria RAM, el resto con 64 GB de memoria RAM y cada host tiene un total de 19,9 GHz de CPU. Desde VMware vCenter Server el administrador del SDDC gestiona los recursos de las VMs de cada componente, monitoriza los recursos del entorno, 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 la infraestructura.

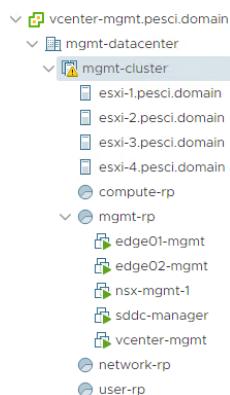


Figura 5.4: Dominio de la instancia de VMware vCenter Server.

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.

## Diseño cluster VMware vSphere

Los cuatro hosts desplegados para el Management Domain están agrupados en un cluster de VMware vSphere, donde se encuentran las VMs de los componentes de VCF (figura 5.4). Gracias a dos funcionalidades de este componente, se establece una configuración para mantener activas las VMs desplegadas dentro de este cluster mediante el balanceo de forma automatizada del consumo de recursos y la recuperación del 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 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 automática y transparente se encarga de monitorizar el estado de las VMs y los 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 vSphere Distributed Switch (vDS), en el cual se configuran puertos a los que se conectan las VMs alojadas en el cluster vSphere.

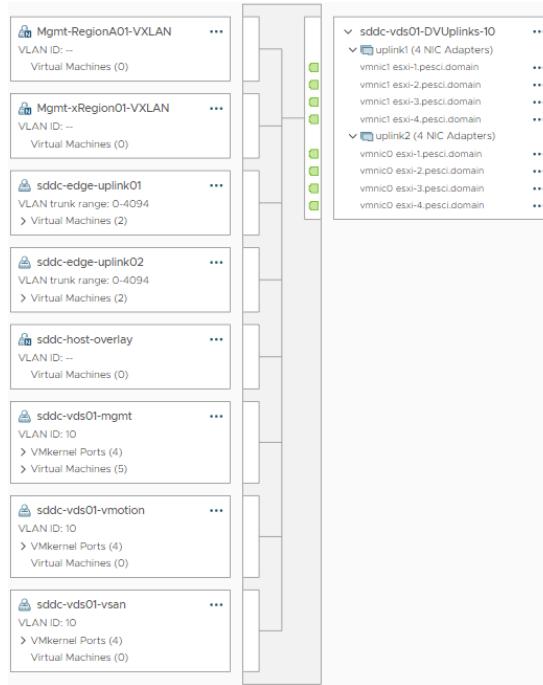


Figura 5.5: Contenido de vSphere Distributed Switch *sddc-vds01*.

Como se muestra en la figura 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-vsxn*, usado por las VMs para acceder al datastore de VMware vSAN, *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-vsxn* y *sddc-vds01-vmotion*, con el fin de asegurarse de que obtienen el suficiente ancho de banda y así facilitar la transmisión de archivos de gran tamaño.

De esta forma, las propiedades del tráfico de cada subred son configuradas a través de VMware vSphere. Esto simplifica el proceso administración y configuración de las subredes 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, la monitorización de la red y la configuración de la calidad del servicio se realizan desde VMware vSphere.

### Diseño almacenamiento VMware vSAN

Los hosts del Management Domain utilizan como almacenamiento un datastore del componente VMware vSAN. Está formado por 16 discos SSD 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.

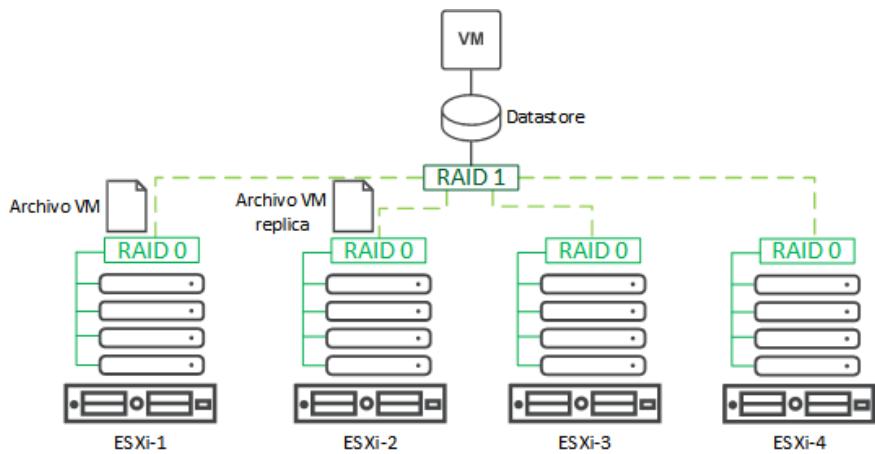


Figura 5.6: Ejemplo de como se almacena un archivo con VMware vSAN y FTT igual a uno

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 del 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 host/grupo de discos mientras la configuración física se mantiene igual.

### Diseño de la red del SDDC con VMware NSX-T

En el entorno de pruebas existe una red virtual que se define mediante software mantenida por VMware NSX-T, que al estar desacoplada de la infraestructura física se puede gestionar sin necesidad de modificar la configuración de la red física. Esto implica que se pueden aplicar diferentes configuraciones de red de forma sencilla, mejorando y simplificando su administración y seguridad. La virtualización de la red con VMware NSX-T se basa principalmente en el concepto de Segment:

- Segment: se trata de un dominio de broadcast de capa 2 (una subred) al cual las VMs se conectan.

Un Segment se extiende por diferentes hosts los cuales pueden estar en la misma red a nivel físico o en distintas partes de la infraestructura. De esta forma, las VMs situadas en hosts con acceso a un Segment pueden conectarse a él y comunicarse de forma directa con otras VMs situadas en un host conectado a una red física diferente. Es decir, con un Segment se pueden comunicar diferentes puntos de la infraestructura sin cambiar la estructura de la red física, ya que VMware NSX-T se encarga de encapsular el tráfico al salir de un host cuando su destino se encuentra en una red física diferente a la de origen, haciendo creer al destinatario que se encuentran en la misma subred.

En el entorno de pruebas existen cuatro Segments, *Mgmt-Region01A-VXLAN* y *Mgmt-xRegion01-VXLAN*, ambos dedicados a dar acceso a la red a los componentes de VMware vRealize Suite y a las VMs desplegadas por los usuarios, y *VCF-edge\_mgmt-cluster\_segment\_11* y *VCF-edge\_mgmt-cluster\_segment\_12*, utilizados para dar salida hacia el router VyOS al tráfico que proviene de los Segments anteriores.

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.

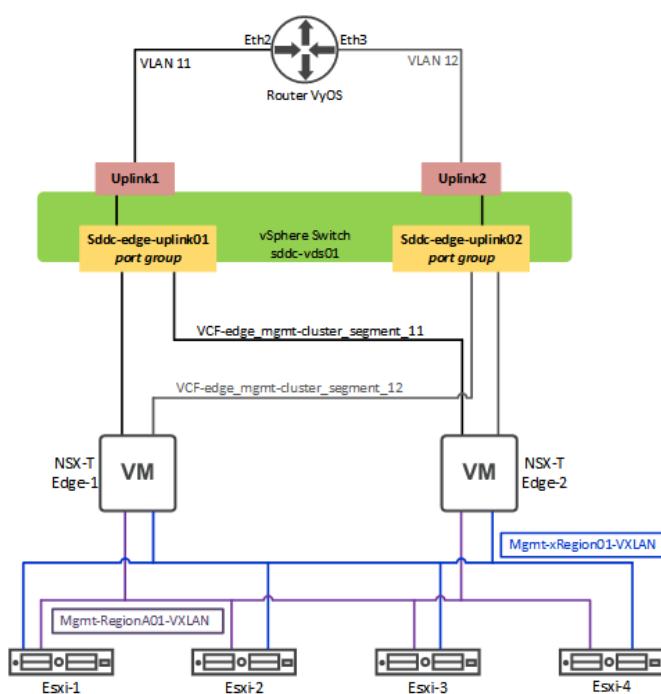


Figura 5.7: Segmentos a los que se conecta cada host del entorno y cómo estos acceden a la red física a través de las VMs de NSX-T Edge.

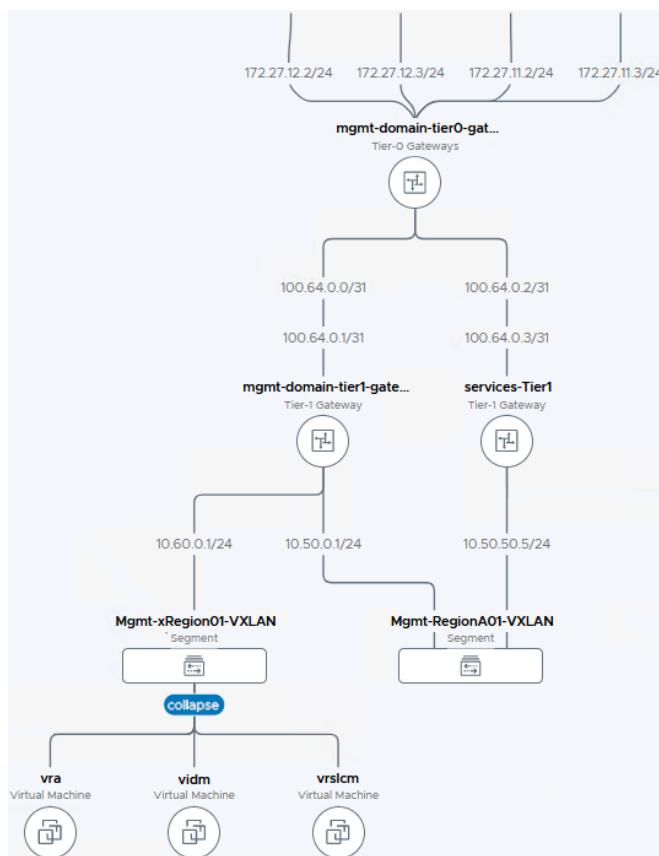


Figura 5.8: Topología virtual de las redes virtuales construidas en VMware NSX-T.

En la primera figura 5.7, 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 física, en última instancia a través del vDS desplegado en el cluster de VMware vSphere. En la segunda figura 5.8, 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 de tipo Tier-1 y uno de tipo Tier-0. Los routers Tier-1 proporcionan servicios de red y enrutamiento entre Segments, *services-Tier1* contiene un servidor DHCP para las VMs que se conecten al Segment *Mgmt-Region01A-VXLAN*, mientras que el router de tipo 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 5.7. Para que el router VyOS tenga conocimiento de las subredes virtuales/Segments existentes, las instancias de NSX-T Edge se las comunica 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 seguridad y establecer servicios dedicados. 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, lo cual implica que una VM se puede migrar de una localización a otra para aumentar su disponibilidad sin necesidad de cambiar su configuración de red. En la infraestructura actual del CITIC todo esto no es posible ya que las redes que se crean dentro del entorno 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 actualmente en el CITIC una plataforma que permita gestionar las redes de la infraestructura de una forma dinámica y sin un alto coste en tiempo y riesgos.

### 5.2.3 Operaciones de la Arquitectura

En este punto ya se ha formado el SDDC, la configuración de la infraestructura física y de todos sus componentes está lista para desplegar los componentes que habiliten el servicio Cloud de aprovisionamiento de recursos. Este último paso se completará con los productos agrupados bajo VMware vRealize Suite. Se utilizarán tres de estos productos, vRealize Suite Lifecycle Manager (vRSLCM), Workspace One Access (WSA) y vRealize Automation (vRA).

#### vRealize Suite Lifecycle Manager

vRSLCM es el primer componente que se instala ya que es el encargado de gestionar el ciclo de vida de los productos de VMware vRealize Suite, incluyendo su despliegue, actuali-

zaciones y gestión de las credenciales de administración, certificados y licencias, por lo tanto permite al administrador del SDDC 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 comunicarse con la instancia de VMware vCenter Server desplegada en el Management Domain.

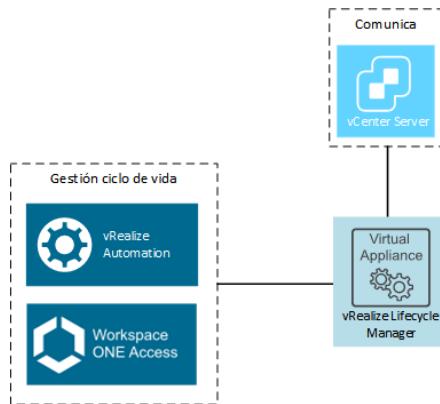


Figura 5.9: Componentes con los que se comunica vRSLCM.

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<sup>5</sup> para habilitar el acceso seguro desde el navegador web. Las instancias de cada componente desplegado se colocan dentro del cluster vSphere<sup>6</sup> creado anteriormente, y utilizarán uno de los Segments creados en VMware NSX-T para conectarse a la red<sup>7</sup>.

<sup>5</sup>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.

<sup>6</sup>Diseño cluster VMware vSphere

<sup>7</sup>Figura 5.8

## CAPÍTULO 5. METODOLOGÍA

---

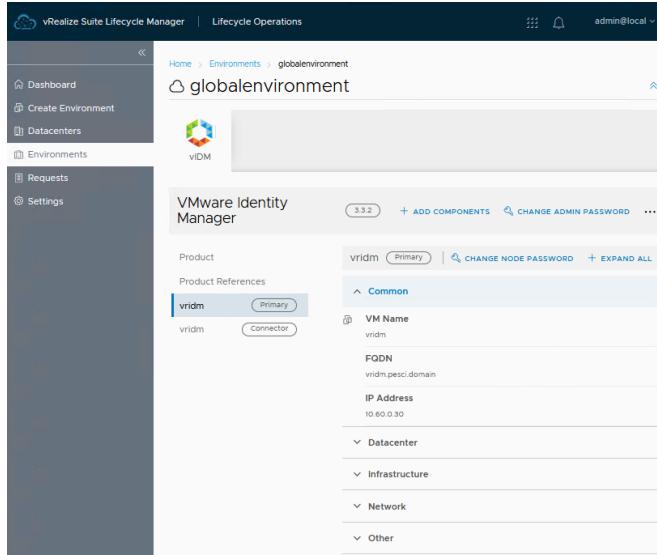


Figura 5.10: Apartado donde se muestra la configuración de la instancia de WSA en vRSLCM.

### Workspace One Access

WSA permite integrar un directorio de usuarios para proporcionarles acceso al servicio Cloud. Así, en el entorno real del CITIC, WSA estaría integrado con el directorio de usuarios de la UDC para que estos pudieran acceder al servicio de aprovisionamiento utilizando las credenciales de la UDC.

En el entorno de pruebas, WSA está integrado 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 quieren sincronizar, para habilitarlos dentro del SDDC y posteriormente configurar su acceso a la plataforma de vRA. Como norma general, los permisos y roles se deben aplicar sobre grupos de usuarios y no a perfiles individuales, de esta forma se reduce el tiempo de gestión y se simplifica la estructura del directorio ya que se configura el acceso de un conjunto de usuarios al mismo tiempo.

Los usuarios configurados en el Active Directory son sincronizados en WSA y serán utilizados para mostrar las funcionalidades del servicio Cloud como si se tratase del entorno en producción. Para realizar la sincronización se seleccionarán las unidades organizativas necesarias.

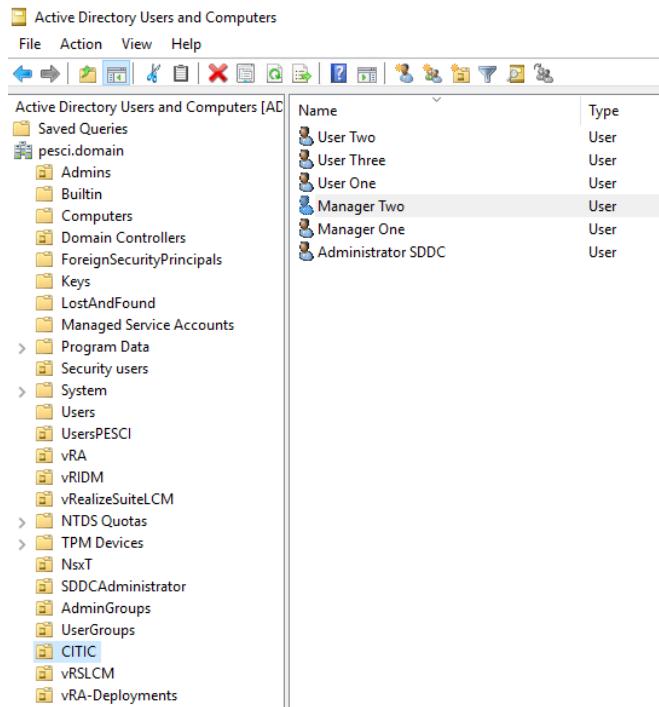


Figura 5.11: Unidades organizativas configuradas en el AD junto a los usuarios pertenecientes a la unidad CITIC.

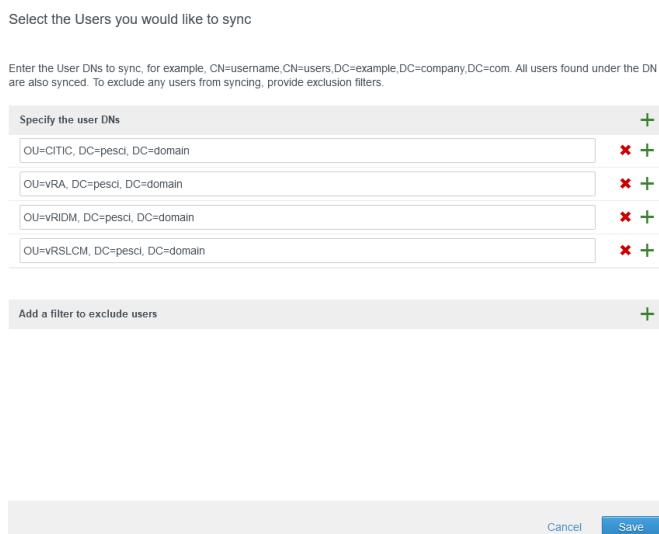
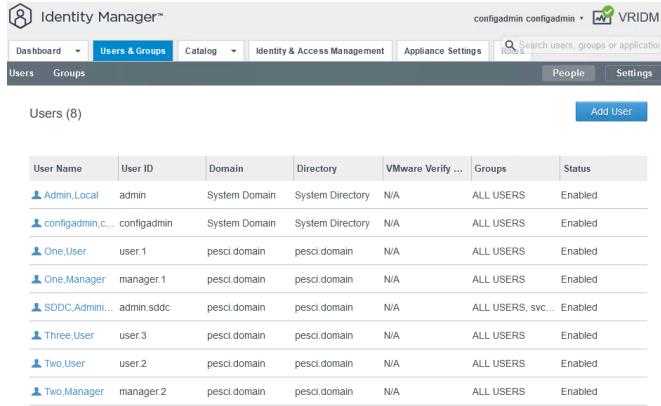


Figura 5.12: Sincronización de usuarios desde Workspace One Access seleccionando Unidades Organizativas.

## CAPÍTULO 5. METODOLOGÍA

---



The screenshot shows the VMware Identity Manager interface. The top navigation bar includes 'Dashboard', 'Users & Groups' (which is selected), 'Catalog', 'Identity & Access Management', 'Appliance Settings', and a search bar. Below the navigation is a sub-menu with 'Users' and 'Groups'. On the right side of the header are user names 'configadmin configadmin' and a VRIDM icon. A search bar at the top right says 'Search users, groups or applications'. The main content area is titled 'Users (8)' and contains a table with the following data:

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_Adminin...	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 5.13: Usuarios sincronizados en Workspace One Access.

El acceso al servicio Cloud está centralizado a través de una plataforma de autenticación proporcionada por WSA. Cuando el usuario intenta acceder al servicio este es redirigido a una página web donde introduce sus credenciales, WSA comprueba los datos introducidos y vuelve a redirigir al usuario a la pantalla del servicio. Utilizando esta plataforma de autenticación el administrador del SDDC puede obtener estadísticas sobre qué usuarios se autentican, a qué servicios acceden y desde dónde lo hacen. Además, también se pueden modificar los parámetros de autenticación y la configuración las sesiones de usuarios, permitiendo definir si el usuario debe utilizar su cuenta de correo electrónico o nombre de usuario para iniciar sesión o si se utilizan cookies de sesión o persistentes. Por si esto fuera poco, también existe la posibilidad de crear políticas para controlar desde dónde pueden los usuarios acceder al servicio y el tiempo de duración de las sesiones. En la siguiente figura se muestran las reglas de la política por defecto que se aplica, en esta se permite el acceso desde cualquier dirección IP, a través de un navegador web, usando su contraseña y con un tiempo de sesión de 8 horas.

## 5.2. Prueba de concepto

The screenshot shows the VMware Identity Manager (VRIDM) interface under the 'Identity & Access Management' tab. A specific policy set named 'default\_access\_policy\_set' is selected. The interface is divided into 'Definition' and 'Configuration' sections. In the 'Definition' section, the name is 'default\_access\_policy\_set' and the description is 'Default access policy set'. Under 'Applications', there is a note '0 Application(s)'. In the 'Configuration' section, there are two policy rules: Rule 1 (if user's network range is ALL RANGES and user is accessing content from Workspace ONE App or Hub App and user belongs to group(s) All Users) and Rule 2 (if user's network range is ALL RANGES and user is accessing content from Web Browser and user belongs to group(s) All Users). Both rules specify authentication via 'Password' and a fallback method of 'Password (Local Directory)'. The configuration also includes a note about re-authentication after 2160 hours.

Figura 5.14: Política de autenticación por defecto establecida en WSA.

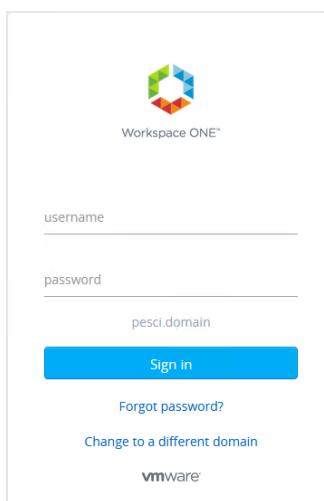


Figura 5.15: Plataforma de autenticación de Workspace One Access.

Con WSA el administrador tiene un mayor control sobre los usuarios y cómo estos acceden al servicio Cloud, ya que desde un único punto se gestionan todos los perfiles de usuarios disponibles y la seguridad de acceso, pudiendo controlar qué usuarios acceden y establecer medidas de seguridad de forma sencilla. La gestión de las credenciales de cada usuario se separa de la gestión del acceso, ya que lo primero está controlado por el AD 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 un perfil manualmente para cada usuario que quiera acceder al servicio y su gestión se centraliza en un componente dedicado a ello.

### 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 elaboran diseños de los recursos que necesitan para posteriormente implementarlos y llevar a cabo sus trabajos. Estos diseños, son archivos con formato .yaml en los que se especifican los recursos de la infraestructura que se quieren utilizar y su configuración, como el tamaño de una VM, su sistema operativo, creación de usuarios, instalación de paquetes, redes a las que se conecta, almacenamiento que utiliza o su localización en la infraestructura. Una vez completado el diseño, el usuario lo ejecuta y vRA se encarga de aprovisionar todos los recursos especificados, de forma ordenada, automatizada y transparente. El administrador del SDDC se encargado de establecer qué recursos de la infraestructura están disponibles para los usuarios, asignando a cada uno un tag con la forma *key:value* para que puedan ser referenciados.

Para separar el flujo de trabajo de diferentes usuarios, vRA permite la creación de proyectos que agrupan a un conjunto de usuarios, en los cuales se habilitan diseños a los que solo los miembros del proyecto tienen acceso. En cada proyecto existe el rol de administrador de proyecto y el de miembro de proyecto, el primero es el que se encarga de determinar qué usuarios tienen acceso al proyecto y de habilitar los diseños en un catálogo, el segundo solo tiene acceso a los proyectos donde ha sido admitido para aprovisionar y utilizar los recursos establecidos en los diseños disponibles. El administrador del SDDC se encarga de la creación de cada proyecto y de establecer recursos la cantidad de recursos disponibles para cada uno.

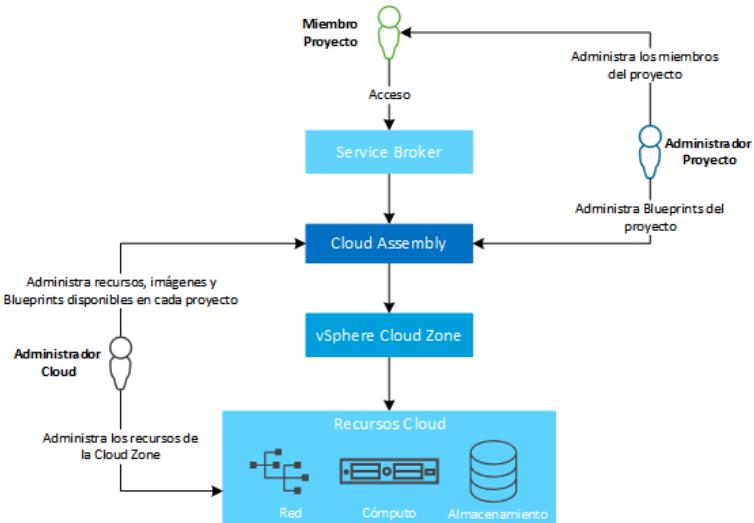


Figura 5.16: Uso y componentes de VMware vRealize Automation.

Como se muestra en la figura anterior, en vRA existen tres componentes principales que son Service Broker, a través del cual los usuarios tienen acceso a los diseños e implemen-

taciones de sus proyectos, Cloud Assembly, donde el administrador del SDDC establece los recursos disponibles y donde los administradores de cada proyecto se elaboran de forma automatizada los diseños, y Cloud Zone, punto desde donde vRA accede a la infraestructura para obtener los recursos.

vRA soluciona las principales carencias de la infraestructura del CITIC y su servicio de virtualización, que son la falta de automatización en el aprovisionamiento y la falta de control sobre el uso y el acceso a los recursos. Con vRA se proporciona un servicio Cloud de tipo IaaS para la obtención de recursos de forma medida y bajo demanda, mientras el administrador del SDDC puede controlar a qué recursos accede cada usuario y cuantos recursos pueden utilizar mediante un servicio de valoración.

En la siguiente sección se detallará como se han configurado los recursos de la infraestructura del entorno de pruebas en vRA y cómo son utilizados por los usuarios, ya que esta será la plataforma que complete el servicio Cloud propuesto para la infraestructura del CITIC.

## 5.2.4 Servicio Cloud

### Preparación de los recursos

El aprovisionamiento de recursos con vRA se traduce en la creación de VMs a partir de plantillas creadas previamente por el administrador del SDDC a las que se les aplica una configuración determinada, y al uso de las subredes y almacenamiento disponibles en la infraestructura.

Con el objetivo de organizar las VMs creadas por los usuarios, en el cluster vSphere del entorno de pruebas se crean una carpeta y un *resource pool* donde se colocarán las nuevas VMs que desplieguen los usuarios, como se muestra en la siguiente figura.

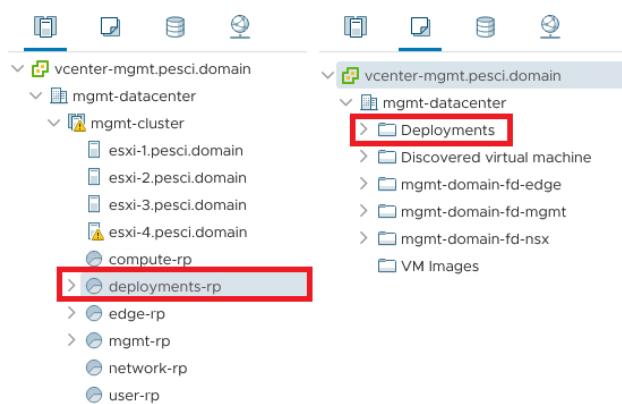


Figura 5.17: Resource pool (izquierda) y carpeta (derecha) creadas para alojar las VMs desplegadas desde vRA.

La red utilizada para dar acceso a las VMs creadas por los usuarios es el Segment *Mgmt-*

## CAPÍTULO 5. METODOLOGÍA

*Region01A-VXLAN* disponible en VMware NSX-T<sup>8</sup>, el cual cuenta con un servidor DHCP<sup>9</sup> y así poder establecer la configuración IP de forma automática de cada nueva VM que se conecte a este Segment.

Segment Name	Connectivity	Transport Zone	Subnets	Ports	Admin State	Status ⓘ
Mgmt-Re...	mgmt-domain-tier1-gateway   Tier1	mgmt-domain-m01-overlay-tz   Overlay	10.50.0.1/24	5	<span>Up</span>	<span>Suc... ⓘ</span>
		DHCP Config	Enabled			
		DHCP Server Address	10.50.50.5/24			
		DHCP Ranges	10.50.0.100-10.50.0.200			
		Lease Time (seconds)	86400			
		DNS Servers	10.0.0.221 and 1 More			

Figura 5.18: Segment utilizado para el despliegue de VMs con vRA (arriba) y la configuración del servidor DHCP definida en VMware NSX-T (abajo)

Para que los usuarios tengan plantillas a partir de las cuales generar sus propias VMs, el administrador del SDDC debe crearlas antes. Este proceso consiste en crear una VM, inicializarla con la instalación de un sistema operativo y establecer una configuración base para finalmente generar una plantilla. En el entorno de pruebas se crean dos plantillas de dos sistemas operativos distintos desde VMware vCenter Server, una con Windows Server 2016 (figura 5.19) y otra con CentOS 8 (figura 5.20). Una vez instalados ambos sistemas se habilita al menos un método de acceso, SSH en el caso de CentOS y RDP en Windows Server, y se instala el servicio **cloud-init**<sup>10</sup> el cual permitirá a los usuarios finales ejecutar comandos de configuración durante el despliegue de una VM para adaptarla a sus requisitos. En sistemas operativos Windows este servicio se llama **cloudbase-init**<sup>11</sup>. Una vez se ha completada la configuración se deben ejecutar una serie de comandos, que en el caso de Windows Server son ejecutados directamente por el instalador de cloudbase-init a través del servicio **sysprep**, para limpiar el sistema y así generar una VM única cada vez que el usuario final utiliza la plantilla. Esto incluye el borrado de paquetes obsoletos y limpieza de logs, claves SSH e identificadores del sistema como direcciones MAC. Una vez se ha completado el proceso se genera una plantilla de cada VM (figura 5.21).

<sup>8</sup>Figura 5.8

<sup>9</sup>Como se observa en la figura 5.18, el servidor DHCP está gestionado por VMware NSX-T ya que forma parte de sus servicios de red.

<sup>10</sup>Ejemplos de uso y su documentación se pueden encontrar en el siguiente enlace: <https://cloudinit.readthedocs.io/en/latest/topics/examples.html>.

<sup>11</sup>Su documentación se puede encontrar en el siguiente enlace: <https://cloudbase.it/cloudbase-init/>.

## 5.2. Prueba de concepto

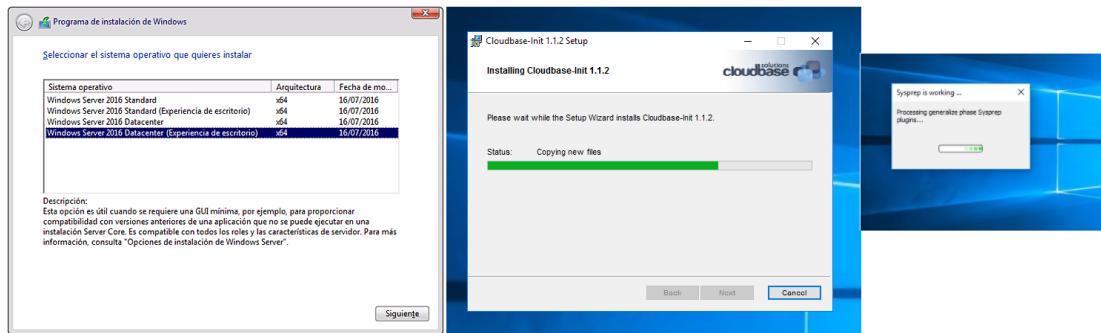


Figura 5.19: Instalación y preparación de la VM con Windows Server 2016 para la creación de una plantilla

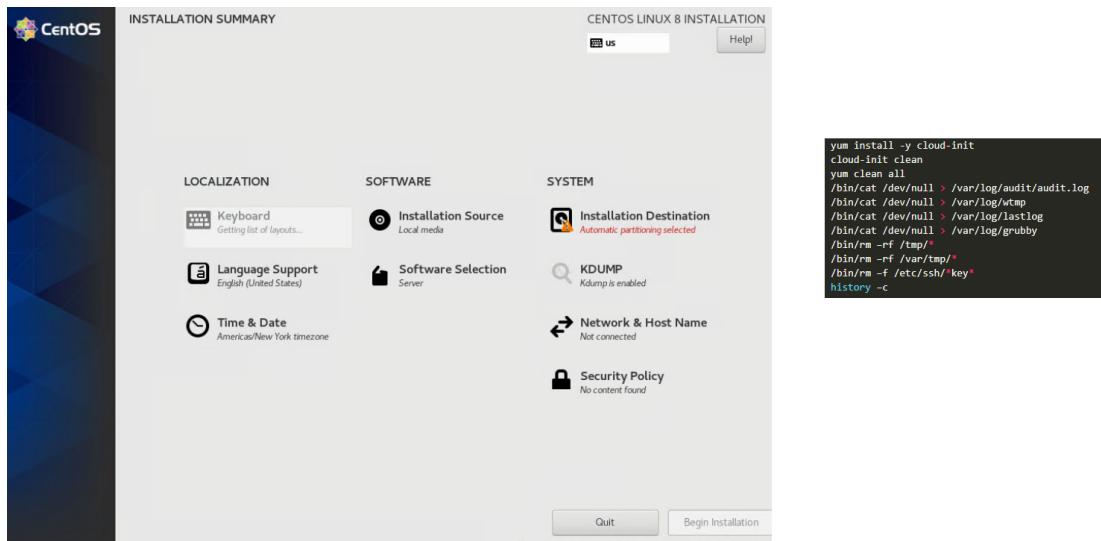


Figura 5.20: Instalación CentOS y comandos ejecutados para la creación de una plantilla.

## CAPÍTULO 5. METODOLOGÍA

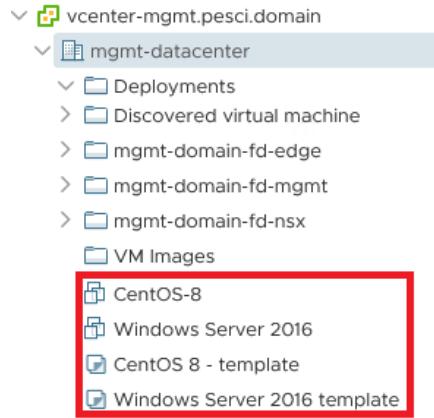


Figura 5.21: Plantillas de CentOS 8 y Windows Server 2016 creadas a partir de sus respectivas VMs.

### Configuración de VMware vRealize Automation

Para que los recursos de cómputo, red y almacenamiento de la infraestructura sean consumidos por los usuarios, es necesario habilitarlos en la plataforma de vRA. A medida que se integra cada recurso se le asigna uno o más tags para poder identificarlo y que el usuario lo pueda incluir en sus diseños.

En la siguiente figura se muestran las plantillas creadas anteriormente en VMware vCenter Server. Cada vez que un usuario quiera crear una VM deberá indicar a partir de qué plantilla quiere generarla.

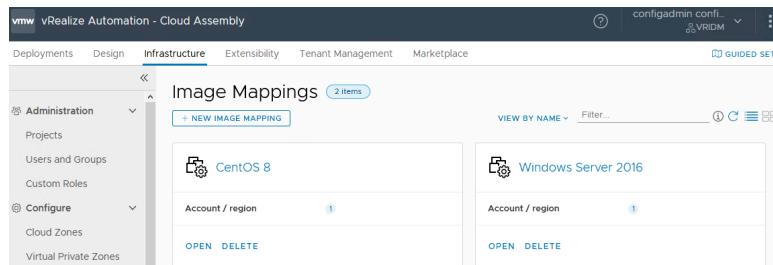


Figura 5.22: Plantillas de CentOS 8 y Windows Server 2016 disponibles en vRA.

Para habilitar el Segment *Mgmt-Region01A-VXLAN*, en vRA se crea un perfil de red y dentro de este se añade la subred deseada. A esta se le asignan los tags *subnet-cidr:10.50.0.0/24*, *function:pro* y *env:pro* como se muestra en la siguiente figura.

The screenshot shows the 'Network-Profile' section in vRA. At the top, there are tabs for 'Summary', 'Networks' (which is selected), 'Network Policies', 'Load Balancers', and 'Security Groups'. Below the tabs, a message states: 'Networks listed here are used when provisioning to existing, on-demand, or public networks.' A button labeled '+ ADD NETWORK' is available. The main table lists one network entry:

Name ↑	Account / Region	Zone ↑	Network Domain ↑	CIDR ↑	Support Public IP ↑	Default for Zone ↑	Origin	Tags
Mgmt-RegionA01-VXLAN	nsxt-management	mgmt-domain-m01-overlay-tz	10.50.0.0/24	4	--	✓	Discover red	subnet-cidr:10.50.0.0/24 policyPath:/infra/segments/l function:pro env:pro

Figura 5.23: Subred habilitada en vRA que se corresponde con el Segment *Mgmt-Region01A-VXLAN* configurado en VMware NSX-T.

Los recursos de cómputo se habilitan configurando una Cloud Zone que se muestra en la figura 5.24. Esta integra en vRA los recursos del cluster vSphere del entorno y permite establecer la política a seguir para escoger el host donde se debe desplegar cada VM<sup>12</sup> y la carpeta y resource pool donde se deben colocar. A esta Cloud Zone se le han asignado los tags *cloud: private* y *region: management*, y al resource pool el tag *resource:rpprivate*.

The screenshot displays two configuration pages. On the left, the 'vSphere-Management / mgmt-datacenter' Cloud Zone configuration page. It includes fields for 'Name' (vSphere-Management / mgmt-datacenter), 'Description' (empty), 'Placement policy' (DEFAULT), and 'Folder' (Deployments). Under 'Capabilities', it lists 'cloud:private' and 'region:management' tags. On the right, the 'mgmt-cluster / deployments-rp' Resource Pool configuration page. It includes fields for 'Name' (mgmt-cluster / deployments-rp), 'Type' (VM\_HOST), and 'Tags' (resource:rpprivate).

Figura 5.24: Cloud Zone (izquierda) y resource pool (derecha) configurados para utilizar los recursos de cómputo y colocar las VMs desplegadas.

Igual que con los recursos de red, para habilitar los recursos de almacenamiento se debe crear un perfil de almacenamiento como se muestra en la figura 5.25. Este perfil integra al datastore vSAN utilizado por el cluster vSphere del entorno y se establece como el perfil por defecto para aprovisionar recursos de almacenamiento desde vRA. Al perfil se le asignan los tags *cloud: private* y *function: pro*.

<sup>12</sup>La opción DEFAULT escoge un host aleatoriamente.

## CAPÍTULO 5. METODOLOGÍA

---

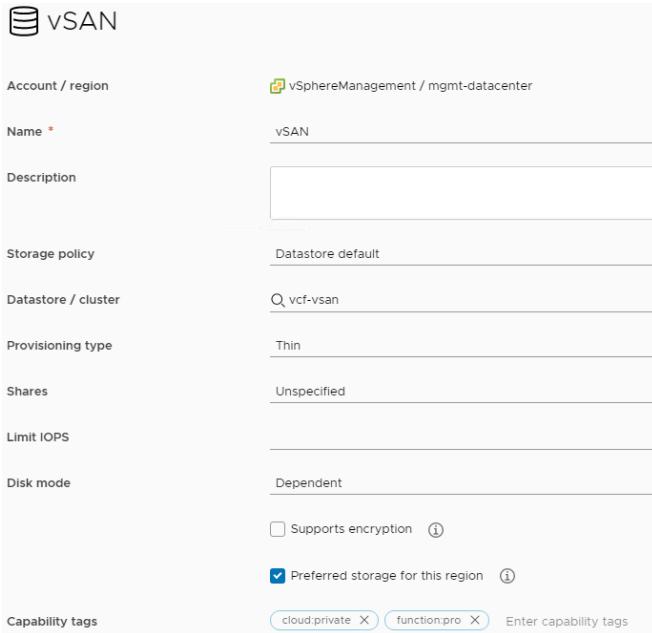


Figura 5.25: Perfil de almacenamiento configurado donde se indica el datastore utilizado para aprovisionar recursos de almacenamiento.

Además, se definen varios perfiles de tamaños para que los usuarios determinen el tamaño de sus VMs. En estos perfiles se define una cantidad de CPU y memoria RAM con el fin de estandarizar la cantidad de recursos que un usuario puede asignar a una VM. En el entorno de pruebas, estos tamaños van desde *x-small* con 1 CPU y 512 MB de memoria RAM, hasta *large* con 8 CPUs y 16 GB de memoria RAM, mostrados en la siguiente figura.

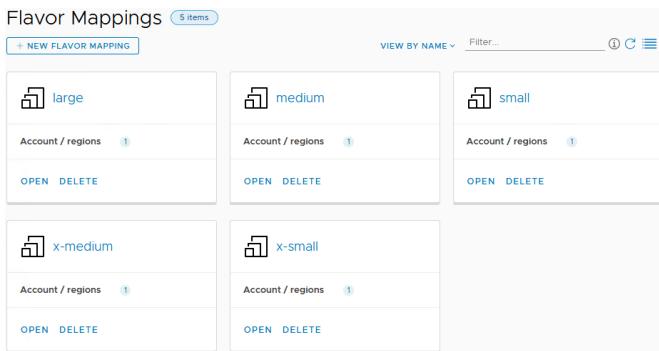


Figura 5.26: Perfiles donde se preestablecen la cantidad de recursos que puede tomar una VM.

Con el objetivo de establecer una valoración de los recursos que utilizan los usuarios, se hace uso de las tarjetas de cobro. Se define una única tarjeta que se aplicará a todos los proyectos que se creen en la plataforma, y a medida que se vayan desplegando VMs se generará un cálculo total en base al precio asignado a cada recurso, a la cantidad de recursos utilizados

y al tiempo que el despliegue se mantiene activo. Tanto el administrador del SDDC como el usuario tendrán acceso a estadísticas sobre el gasto que se realiza y de la cantidad total de recursos utilizados. En la figura 5.27 se muestra la valoración establecida para el consumo de recursos, que es de 1 €/hora por cada CPU cuando la VM está encendida, 2 €/hora por cada GB de memoria RAM cuando la VM está encendida y 0,5 €/hora por GB de almacenamiento mientras el despliegue esté activo.

The screenshot shows a pricing card for a deployment named "Precio-Despliegue". The card has tabs for "Summary", "Pricing", and "Assignments", with "Summary" selected. It includes fields for Name (Precio-Despliegue), Description (empty), Currency (EUR), and a checkbox for "Default for unassigned projects?". Below this is an "Overview" section with a table of resource charges:

Type	Value	Description
Basic Charges	vCPU	€1.00 per vCPU hourly, only when powered on
	Memory	€2.00 per GB hourly, only when powered on
	Storage	€0.50 per GB hourly, always

Figura 5.27: Tarjeta de cobro para valorar los recursos consumidos por los usuarios.

## Uso del servicio Cloud

La plataforma de vRA ya está lista para ser utilizada por los usuarios. Los usuarios del CITIC que la utilizarán se organizan en proyectos, donde existe al menos un coordinador o administrador de proyecto. Cuando un grupo de usuarios quiere utilizar el servicio Cloud primero debe comunicarlo al administrador del SDDC, el cual crea el proyecto correspondiente y habilita el acceso a cada usuario con sus correspondientes permisos.

Como ya se ha visto en la sección [Workspace One Access](#), en el entorno de pruebas se han configurado cinco usuarios que se dividen en dos proyectos, uno llamado Web-DB con el objetivo de que los usuarios pertenecientes puedan construir un sitio web bajo demanda, y otro llamado Server-Desktop donde sus integrantes puedan desplegar dos VMs para realizar cierto trabajo de investigación (figura 5.28). El proyecto Web-DB lo forman el usuario *User One*, *User*

## CAPÍTULO 5. METODOLOGÍA

*Two* y *Manager One*, el cual es el coordinador del grupo, y el proyecto Server-Desktop está formado por *User Two*, *User Three* y *Manager Two*, el cual será el coordinador de este segundo grupo. Entonces, a los usuarios *Manager One* y *Manager Two* se les asigna el rol Administrador de Proyecto, y al resto de usuarios el rol Miembro de Proyecto, los primeros podrán controlar los diseños disponibles en el catálogo del proyecto, qué usuarios tienen acceso y los despliegues que estos realicen, mientras que los miembros del proyecto podrán desplegar los diseños habilitados (figura 5.28).

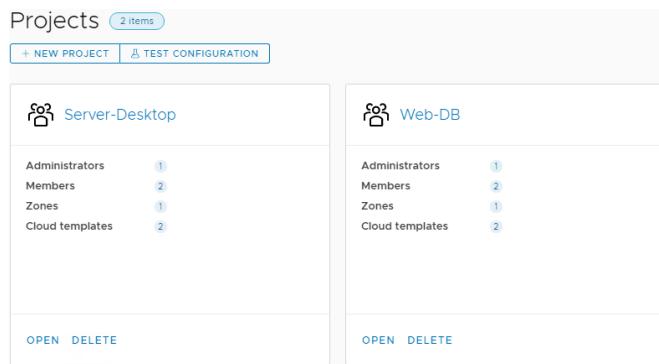


Figura 5.28: Proyectos creados para dar acceso a los usuarios a vRA.

<input type="checkbox"/>	Name	Account	Role
<input type="checkbox"/>	Manager Two	manager_2	Administrator
<input type="checkbox"/>	User Three	user_3	Member
<input type="checkbox"/>	User Two	user_2	Member

Name	Account	Role
Manager One	manager_1	Administrator
User One	user_1	Member
User Two	user_2	Member

Figura 5.29: Usuarios del proyecto Server-Desktop (izquierda) y usuarios del proyecto Web-DB (derecha).

Durante la creación de los proyectos el administrador establece la cantidad máxima de CPU, memoria RAM y almacenamiento que pueden consumir en total los usuarios del proyecto. Como se trata de un entorno de pruebas en el proyecto Server-Desktop se establece un límite de 2 VMs, 10 GB de memoria RAM y 6 CPUs, y en el proyecto Web-DB un límite de 3 VMs, 10 GB de memoria RAM y 6 CPUs, de esta forma los usuarios del proyecto no podrán superar ninguno de los límites establecidos. Para obtener una valoración del consumo se asigna a cada proyecto la tarjeta de cobro creada anteriormente.

Una vez configurados ambos proyectos los administradores de cada uno pueden acceder y empezar a crear los diseños de los recursos que requieran sus usuarios a través del componente Cloud Assembly. El administrador del proyecto Server-Desktop, *Manager Two*, crea el diseño con el nombre WD-Server que se muestra en la siguiente figura<sup>13</sup>.

<sup>13</sup>En el anexo A.1 se encuentra el contenido del archivo .yaml donde se establece la configuración del diseño.

## 5.2. Prueba de concepto

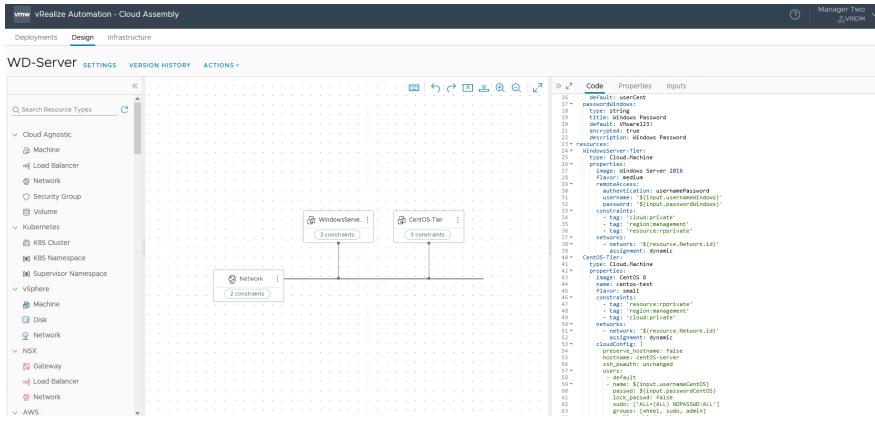


Figura 5.30: Diseño WD-Server para el proyecto Server-Desktop.

En el archivo .yaml del diseño WD-Server se define una VM con el sistema operativo Windows Server 2016 y otra con CentOS 8, y una red a la que ambas se conectan. Se establecen además unas credenciales para cada VM, cuyos datos son introducidos por el usuario cuando se despliega el diseño y así poder iniciar sesión en ellas mediante SSH, o RDP en el caso de Windows. Los tags que se utilizan en la definición de las VMs son *cloud:private*, *region:management* y *resource:rpprivate*, y el tag *subnet-cidr:10.50.0.0/24* en la definición de la red, por lo tanto ambas VMs utilizarán los recursos del cluster vSphere, el Segment definido en VMware NSX-T y el datastore vSAN del entorno. En cuanto a la configuración de las interfaces de red, se establece que se configuren de forma dinámica con el servidor DHCP disponible en el Segment. Una vez completado el diseño, *Manager Two* publica el diseño en el catálogo del proyecto para que los usuarios puedan acceder a él. Durante la publicación se especifica la versión del diseño ya que este puede ser actualizado, como se muestra en la siguiente figura.

## CAPÍTULO 5. METODOLOGÍA

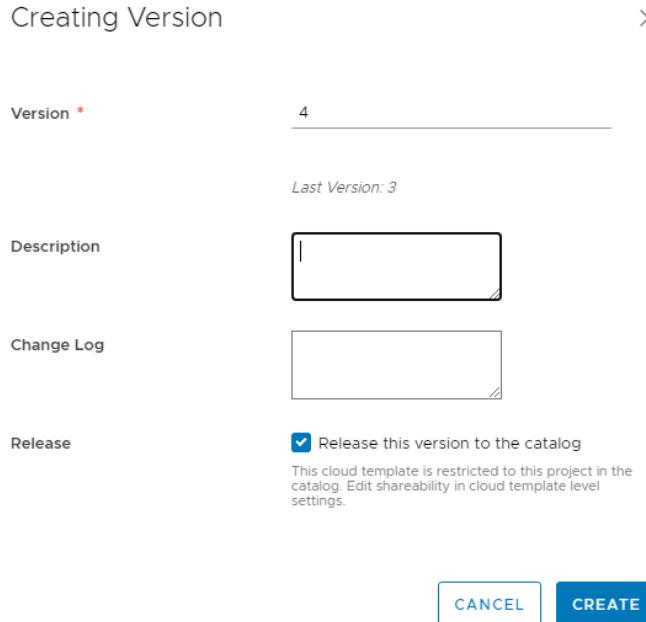


Figura 5.31: Publicación en el catálogo de una nueva versión del diseño.

De la misma forma que para el proyecto Server-Desktop, el administrador del proyecto Web-WD, *Manager One*, crea el diseño de los recursos necesarios para que los usuarios del proyecto puedan generar un sitio web basado en Wordpress automatizando la configuración del entorno, con la idea de que una vez desplegados los recursos el usuario pueda trabajar inmediatamente y exclusivamente en su sitio web. En la siguiente figura se muestra el diseño creado para el proyecto Web-WD<sup>14</sup>.

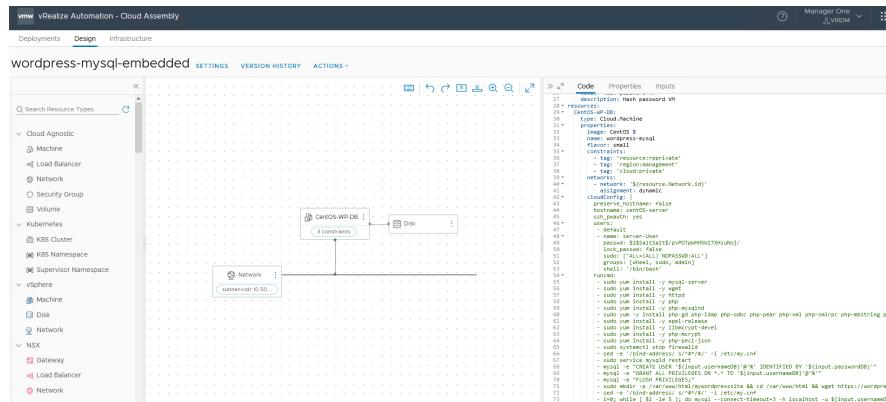


Figura 5.32: Diseño Wordpress-MySQL-Embedded para el proyecto Web-WD.

En el archivo .yaml del diseño Wordpress-MySQL-Embedded se define una VM con el

<sup>14</sup>En el anexo A.2 se encuentra el contenido del archivo .yaml donde se establece la configuración del diseño.

sistema operativo CentOS 8, una red a la cual se conecta y un disco de almacenamiento conectado a la VM. En la sección **cloudConfig** del diseño se definen una serie de comandos que se ejecutan durante la inicialización de la VM cuando se despliega. Estos comandos son ejecutados por el servicio **cloud-init** y con ellos primero se instalan los paquetes necesarios para ejecutar MySQL y el framework Wordpress en un servidor Apache, luego se crea una base de datos y se configura Wordpress. De esta forma una vez se complete un despliegue el sitio web estará listo para ser usado. Además también se incluyen en esa sección del diseño los atributos que permiten a cloud-init crear las credenciales para acceder a la VM mediante SSH. Este diseño utiliza los mismos tags que el proyecto Server-Desktop por lo tanto utilizará los mismos recursos de cómputo, red y almacenamiento. Finalmente, *Manager One* publica el diseño en el catálogo.

Una vez completada la fase de diseño y publicación, los usuarios ya pueden acceder a la plataforma Cloud y comenzar a utilizar los recursos en base a los diseños disponibles. A continuación se muestra cómo los usuarios de cada proyecto acceden al servicio Cloud y utilizan los recursos. El usuario *User Three* perteneciente al proyecto Server-Desktop accede a la plataforma utilizando sus credenciales<sup>15</sup>, una vez inicia sesión accede al componente Service Broker de vRA donde se le muestra el catálogo de diseños disponibles en el proyecto al que pertenece (figura 5.33). Cuando inicia el despliegue del diseño WD-Server, se muestra un formulario donde introduce los datos de las credenciales de cada VM<sup>16</sup> que se va a crear y el nombre del despliegue (figura 5.34). A continuación comienza el proceso de despliegue. En este punto vRA se encarga de crear, configurar y reservar los recursos descritos en el diseño sin que el usuario tenga que realizar ninguna operación adicional (figura 5.35).

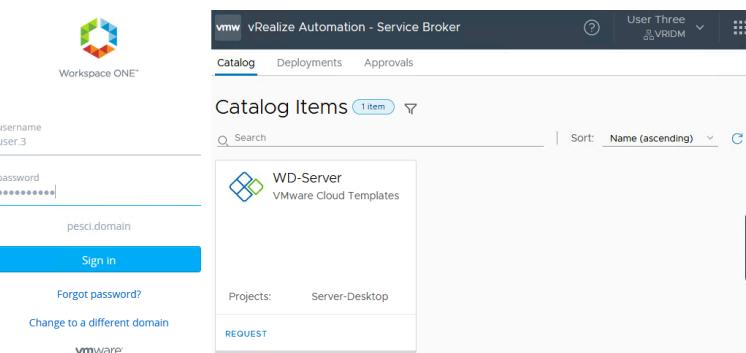


Figura 5.33: Inicio de sesión del usuario *User Three* (izquierda) y catálogo de diseños disponibles en el proyecto Server-Desktop (derecha).

<sup>15</sup>En el caso del entorno real utilizaría sus credenciales de la UDC.

<sup>16</sup>Para la VM con CentOS es necesario indicar el hash de la contraseña ya que el SO lo interpreta de esta forma, generado en este caso con el comando `openssl passwd -1 -salt SaltSalt VMware123!` desde el powershell de Windows siendo "VMware123!" la contraseña en texto plano.

## CAPÍTULO 5. METODOLOGÍA

The screenshot shows the vRealize Automation - Service Broker interface. At the top, it says "vmw vRealize Automation - Service Broker" and "User Three". Below that, there are tabs for "Catalog", "Deployments", and "Approvals", with "Catalog" being the active tab. The main area is titled "New Request" and shows a "WD-Server" template with version 3 selected. The form fields include:

- Project \***: Server/Desktop
- Deployment Name \***: User3-Work
- Description**: (empty text area)
- CentOS Password (hash) \***: \$1\$SaltSalt\$/pvPOTpWHH5W17XHzuNoj/
- CentOS username**: userCent
- Windows Password**: (redacted)
- Windows username**: userCent

At the bottom are two buttons: "SUBMIT" and "CANCEL".

Figura 5.34: Formulario para configurar el nuevo despliegue iniciado por el usuario *User Three*.

The top screenshot shows the "Deployments" page with one item. It displays a deployment for "User3-Work" with the status "Create - In Progress". The details show:

- Requestor: user.3
- Project: Server/Desktop
- Cloud Template: WD-Server, version: 3
- Expires on: Never
- Last updated: Oct 28, 2020, 12:36:59 PM
- Created on: Oct 28, 2020, 12:35:53 PM

The bottom screenshot shows the "History" tab for the same deployment. It lists the following events:

Timestamp	Status	Resource type	Resource name	Details
Oct 28, 2020, 12:36:59 PM	CREATE_IN_PROGRESS	Cloud Machine	WindowsServer-Tier	Request is in stage STARTED and substage RESOURCE_COUNTED
Oct 28, 2020, 12:36:59 PM	CREATE_IN_PROGRESS	Cloud Machine	CentOS-Tier	Request is in stage STARTED and substage RESOURCE_COUNTED
Oct 28, 2020, 12:36:59 PM	CREATE_IN_PROGRESS	Cloud Machine	WindowsServer-Tier	
Oct 28, 2020, 12:36:59 PM	CREATE_IN_PROGRESS	Cloud Machine	CentOS-Tier	
Oct 28, 2020, 12:36:59 PM	CREATE_FINISHED	Cloud Network	Network	Cloud Resource Name: Mgmt-

There are 17 Events listed in total.

Figura 5.35: Tarjeta del despliegue iniciado por el usuario *User Three* (arriba) y la monitorización de todas las tareas llevadas a cabo por vRA durante el despliegue (abajo).

Cuando la creación y configuración de los recursos se ha completado estos ya están listos para su uso. En el panel de control del despliegue se muestra información como direcciones IP de las VMs, discos de almacenamiento disponibles en cada VM, la configuración aplicada a las VMs durante el despliegue o las credenciales indicadas por el usuario para acceder a las VMs (figura 5.36). Además, desde este punto es donde el usuario puede gestionar los recursos pudiendo encenderlos o apagarlos, añadir discos de almacenamiento, modificar el tamaño de la VM, crear copias de seguridad y añadir tags para cambiar la ubicación de los recursos (figura 5.37). Para acceder a las VMs creadas, *User Three* simplemente tiene que comprobar las direcciones IP que se han asignado y conectarse a la VMs mediante SSH o a través de un cliente de escritorio remoto en el caso de Windows Server 2016 (figura 5.38).

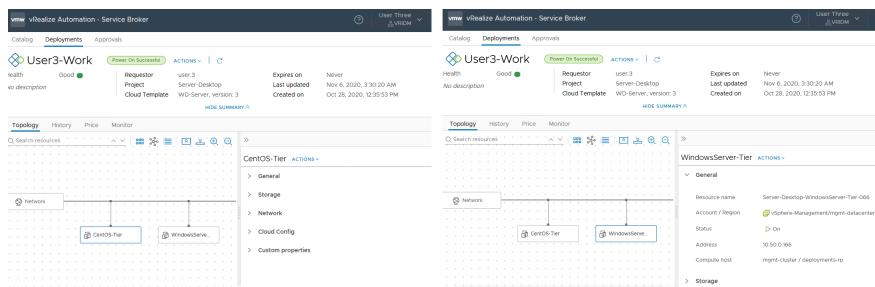


Figura 5.36: Panel de control de la VM CentOS creada por *User Three* (izquierda) y panel de control de la VM Windows creada por *User Three* (derecha).

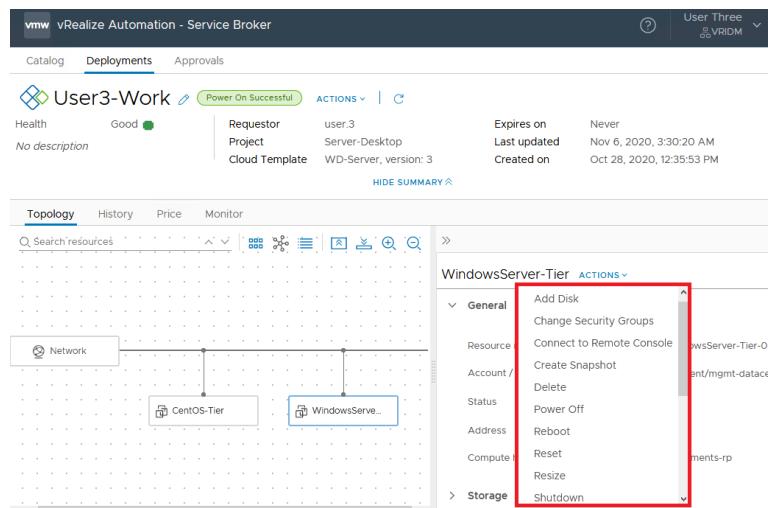


Figura 5.37: Acciones que *User Three* puede ejecutar sobre las VMs creadas.

## CAPÍTULO 5. METODOLOGÍA

---

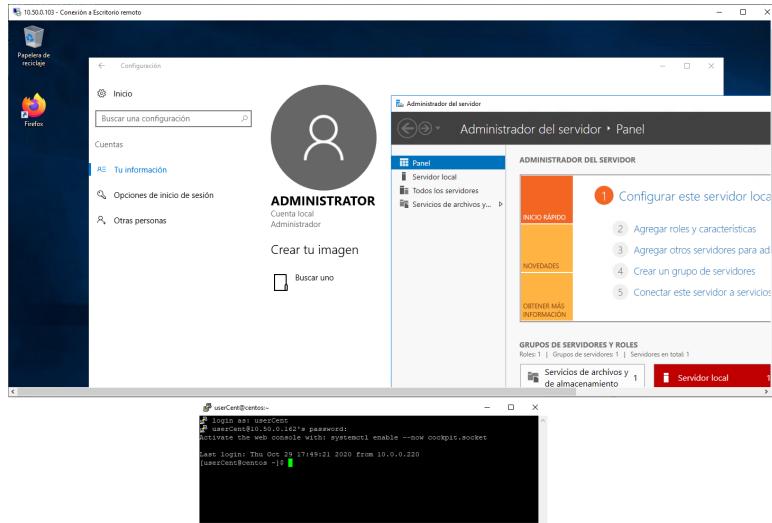


Figura 5.38: Conexión de *User Three* mediante RDP a la VM con Windows Server 2016 (arriba) y mediante SSH a la VM con CentOS (abajo).

En el proyecto Web-WD, el usuario *User Two* accede a la plataforma de vRA y en el catálogo tiene disponibles dos diseños, WD-Server y Wordpress-MySQL-Embedded, ya que es miembro de los dos proyectos Server-Desktop y Web-WD (figura 5.39). El objetivo de este usuario es montar un sitio web por lo tanto inicia el despliegue del diseño Wordpress-MySQL-Embedded. En el formulario de configuración *User Two* introduce las credenciales que se deben configurar en la VM para acceder a ella y para configurar a la base de datos (figura 5.39), luego inicia el despliegue del diseño (figura 5.40). Una vez generada la VM con CentOS el servicio cloud-init se inicia y ejecuta los comandos descritos en el diseño (figura 5.41). Cuando este proceso se ha completado el usuario ya puede acceder al panel de control del despliegue (figura 5.42), comprobar la dirección IP de la VM, acceder a Wordpress a través del navegador, realizar la configuración inicial de su sitio web y comenzar a editar artículos (figura 5.43).

## 5.2. Prueba de concepto

The screenshot shows two side-by-side views of the vRealize Automation - Service Broker interface. On the left, the 'Catalog' tab is selected, displaying 'Catalog Items (2 items)'. It lists two items: 'WD-Server VMware Cloud Templates' (Project: Server/Desktop, Status: REQUEST) and 'wordpress-mysql-embedded VMware Cloud Templates' (Project: Web-DB, Status: REQUEST). On the right, the 'New Request' form is open for the 'wordpress-mysql-embedded' template. The form fields include: Project: 'Web-DB', Deployment Name: (empty), Description: (empty), Database Password: '\*\*\*\*\*', Hash password VM: '\$1\$salt\$pwPOTpWhDW7XhbuNq', Database Username: 'user01', and Username VM: 'server<User'. At the bottom are 'SUBMIT' and 'CANCEL' buttons.

Figura 5.39: Diseños disponibles para *User Two* (izquierda). Formulario de configuración de un nuevo despliegue del diseño Wordpress-MySQL-Embedded (derecha).

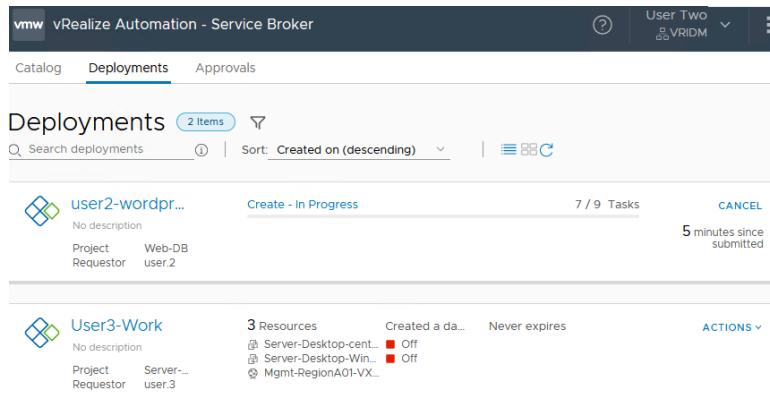


Figura 5.40: Despliegues user2-wordpress-blog iniciado por *User Two*.

## CAPÍTULO 5. METODOLOGÍA

```
=====
Install 1 Package
Total download size: 73 k
Installed size: 44 k
Downloading Packages:
php-json-7.2.24-1.module_el8.2.0+313+b04d0a66.x 14 kB/s | 73 kB     00:05
-----
Total                                         6.7 kB/s | 73 kB     00:10
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing : 1/1
  Installing : php-json-7.2.24-1.module_el8.2.0+313+b04d0a66.x86_64 1/1
  Running scriptlet: php-json-7.2.24-1.module_el8.2.0+313+b04d0a66.x86_64 1/1
  Verifying   : php-json-7.2.24-1.module_el8.2.0+313+b04d0a66.x86_64 1/1
Installed:
  php-json-7.2.24-1.module_el8.2.0+313+b04d0a66.x86_64

Complete!
Redirecting to /bin/systemctl restart mysqld.service
--2020-10-29 12:29:20-- https://wordpress.org/latest.tar.gz
Resolving wordpress.org (wordpress.org)... 198.143.164.252
Connecting to wordpress.org (wordpress.org)|198.143.164.252|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12983648 (12M) [application/octet-stream]
Saving to: 'latest.tar.gz'
```

Figura 5.41: Fragmento de la ejecución de cloud-init donde se instala el paquete php-json y se descargan los archivos para la instalación de Wordpress.

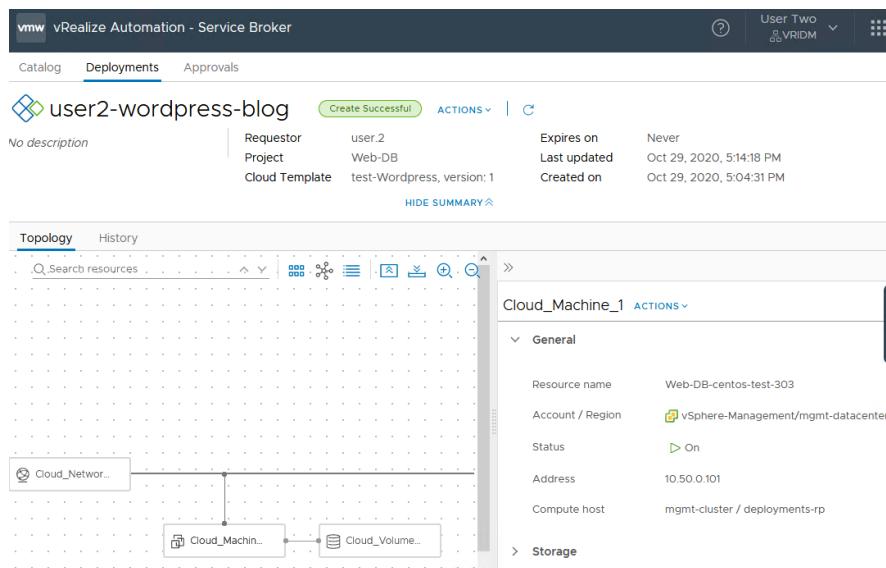


Figura 5.42: Panel de control del despliegue iniciado por *User Two* una vez finalizado.

## 5.2. Prueba de concepto

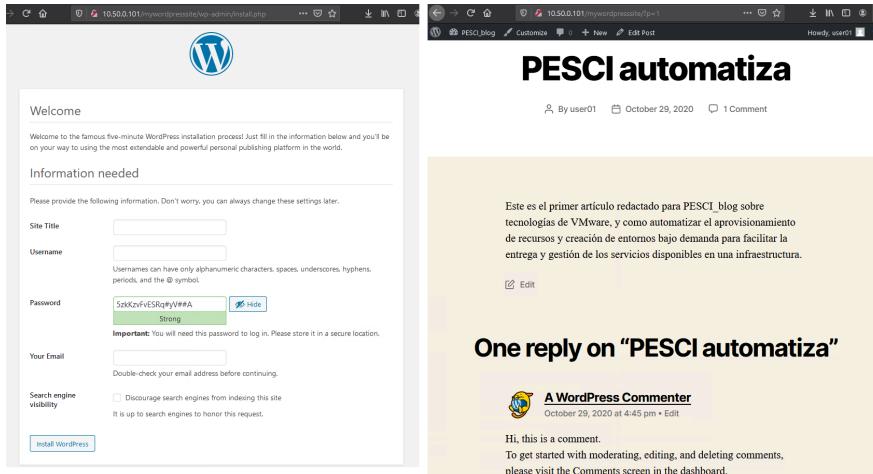


Figura 5.43: Página de instalación de Worpress cuando *User Three* accede por primera vez (izquierda). Primer artículo escrito por *User Two* en su nuevo sitio web.

A medida que se despliegan los diseños las VMs creadas comienzan a consumir recursos. El administrador del SDDC y los usuarios pueden monitorizar el consumo desde el panel de control de cada despliegue, donde pueden acceder a estadísticas diarias, semanales y mensuales sobre el uso de CPU, memoria RAM, almacenamiento y red.

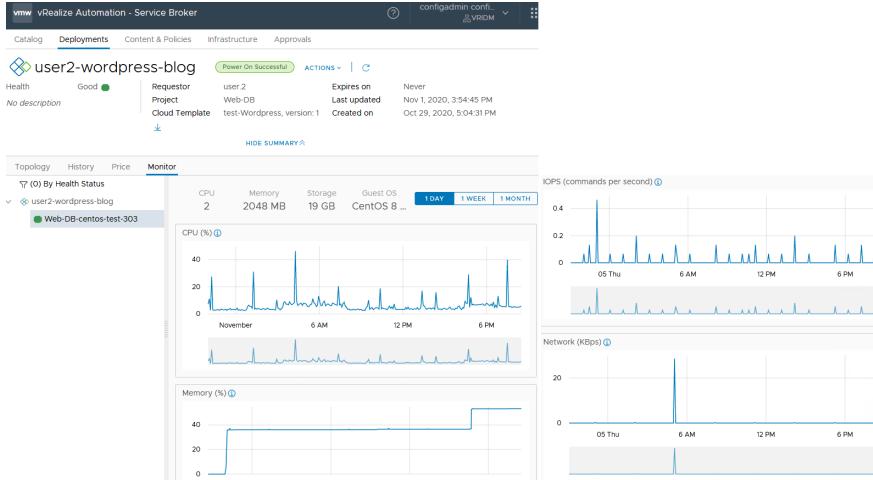


Figura 5.44: Panel de control del despliegue User2-Wordpress-Blog con la vista de monitorización de la VM Web-DB-CentOS-test-303.

Las estadísticas en cuanto a la valoración de los recursos en base a la tarjeta de cobro establecida también es accedida desde el panel de control del despliegue bajo la pestaña "Price". En ella los usuarios pueden ver la valoración total diaria, semanal y mensual de los recursos consumidos en el despliegue, y también de forma detallada donde se desglosa la valoración total en la valoración del cómputo, almacenamiento y otros cargos adicionales que se pue-

## CAPÍTULO 5. METODOLOGÍA

---

dan aplicar. Además, el administrador del SDDC también tiene acceso a estadísticas sobre la valoración total sobre el consumo de recursos de un proyecto.

De esta forma el administrador del SDDC puede asignar a cada proyecto o usuario una cuenta con una cantidad de dinero ficticio del la cual se vaya extrayendo de forma mensual o semanal la valoración del consumo de recursos realizada por la plataforma. Cuando la cuenta esté vacía o no tenga suficiente saldo para consumir más recursos el administrador del SDDC puede bloquear nuevos despliegues dentro del proyecto o del usuario correspondiente hasta que su cuenta vuelva a tener saldo, para así conseguir que haya recursos disponibles para todos los usuarios y evitar que se mantengan despliegues activos cuyas VMs no están siendo usadas.



# **Apéndices**



## Apéndice A

# Material adicional

---

### A.1 Diseño WD-Server para vRealize Automation

Diseño elaborado para desplegar una VM con Windows Server 2016 y otra VM con CentOS 8 sobre una misma red en VMware vRealize Automation.

```
1 formatVersion: 1
2 inputs:
3   usernameCentOS:
4     type: string
5     title: CentOS username
6     description: CentOS username
7     default: userCent
8   passwordCentOS:
9     type: string
10    title: CentOS Password (hash)
11    description: Hash de la contraseña CentOS
12   usernameWindows:
13     type: string
14     title: Windows username
15     description: Windows username
16     default: userCent
17   passwordWindows:
18     type: string
19     title: Windows Password
20     default: VMware123!
21     encrypted: true
22     description: Windows Password
23 resources:
24   WindowsServer-Tier:
25     type: Cloud.Machine
26     properties:
27       image: Windows Server 2016
```

```

28 flavor: medium
29 remoteAccess:
30     authentication: usernamePassword
31     username: '${input.usernameWindows}'
32     password: '${input.passwordWindows}'
33 constraints:
34     - tag: 'cloud:private'
35     - tag: 'region:management'
36     - tag: 'resource:rpprivate'
37 networks:
38     - network: '${resource.Network.id}'
39         assignment: dynamic
40 CentOS-Tier:
41     type: Cloud.Machine
42     properties:
43         image: CentOS 8
44         name: centos-test
45         flavor: small
46         constraints:
47             - tag: 'resource:rpprivate'
48             - tag: 'region:management'
49             - tag: 'cloud:private'
50 networks:
51     - network: '${resource.Network.id}'
52         assignment: dynamic
53 cloudConfig: |
54     preserve_hostname: false
55     hostname: centOS-server
56     ssh_pauth: unchanged
57 users:
58     - default
59     - name: ${input.usernameCentOS}
60         passwd: ${input.passwordCentOS}
61         lock_passwd: false
62         sudo: [ 'ALL=(ALL) NOPASSWD:ALL' ]
63         groups: [wheel, sudo, admin]
64         shell: '/bin/bash'
65 Network:
66     type: Cloud.Network
67     properties:
68         networkType: existing
69     constraints:
70         - tag: 'subnet-cidr:10.50.0.0/24'
71         - tag: 'cloud:private'
```

## A.2 Diseño Wordpress-MySQL-Embedded para vRealize Automation

Diseño elaborado para desplegar una VM con CentOS 8 y el framework Wordpress preparado para crear un sitio web.

```
1 formatVersion: 1
2 inputs:
3   usernameDB:
4     type: string
5     minLength: 4
6     maxLength: 20
7     pattern: '[a-z]+'
8     default: user01
9     title: Database Username
10    description: Database Username
11   passwordDB:
12     type: string
13     pattern: '[a-zA-Z0-9@#$]+'
14     default: password
15     encrypted: true
16     title: Database Password
17     description: Database Password
18   usernameVM:
19     type: string
20     default: user01
21     title: Username VM
22     description: Username VM
23   passwordVM:
24     type: string
25     default: $1$SaltSalt$/pvPOTpWHH5W17XHzuNoj/
26     title: Hash password VM
27     description: Hash password VM
28 resources:
29   Cloud_Machine_1:
30     type: Cloud.Machine
31     properties:
32       image: CentOS 8
33       name: centos-test
34       flavor: small
35     constraints:
36       - tag: 'resource:rpprivate'
37       - tag: 'region:management'
38       - tag: 'cloud:private'
39     networks:
```

```

40      - network: '${resource.Cloud_Network_1.id}'
41          assignment: dynamic
42      cloudConfig: |
43          preserve_hostname: false
44          hostname: centOS-server
45          ssh_pauth: yes
46      users:
47          - default
48          - name: server-User
49              passwd: $1$SaltSalt$/pvPOTpWHH5W17XHzuNoj/
50              lock_passwd: false
51              sudo: [ 'ALL=(ALL) NOPASSWD:ALL' ]
52              groups: [wheel, sudo, admin]
53              shell: '/bin/bash'
54      runcmd:
55          - sudo yum install -y mysql-server
56          - sudo yum install -y wget
57          - sudo yum install -y httpd
58          - sudo yum install -y php
59          - sudo yum install -y php-mysqlnd
60          - sudo yum -y install php-gd php-ldap php-odbc php-pear
61          - sudo yum -y install php-xml php-xmlrpc php-mbstring php-snmp php-soap curl
62          - sudo yum install -y epel-release
63          - sudo yum install -y libmcrypt-devel
64          - sudo yum install -y php-mcrypt
65          - sudo yum install -y php-pecl-json
66          - sudo systemctl stop firewalld
67          - sed -e '/bind-address/ s/^#*/#/ -i /etc/my.cnf
68          - sudo service mysqld restart
69          - mysql -e "CREATE USER '${input.usernameDB}'@'%'"
70          IDENTIFIED BY '${input.passwordDB}'"
71          - mysql -e "GRANT ALL PRIVILEGES ON *.* TO
72          '${input.usernameDB}'@'%'"
73          - mysql -e "FLUSH PRIVILEGES;"
74          - sudo mkdir -p /var/www/html/mywordpresssite && cd
75          /var/www/html && wget https://wordpress.org/latest.tar.gz && tar
-xzf /var/www/html/latest.tar.gz -C
/var/www/html/mywordpresssite --strip-components 1
    - sed -e '/bind-address/ s/^#*/#/ -i /etc/my.cnf
    - i=0; while [ $i -le 5 ]; do mysql --connect-timeout=3 -h
localhost -u ${input.usernameDB} -p${input.passwordDB} -e "SHOW
STATUS;" && break || sleep 15; i=$((i+1)); done
    - mysql -u ${input.usernameDB} -p${input.passwordDB} -h
localhost -e "create database wordpress_blog;"
    - sudo cp /var/www/html/mywordpresssite/wp-config.php
/var/www/html/mywordpresssite/wp-config-sample.php

```

## APÉNDICE A. MATERIAL ADICIONAL

---

```
76      - sed -i -e s/"define( 'DB_NAME', 'database_name_here' )%;" /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define( 'DB_USER', 'username_here' );%;" /"define( 'DB_USER', '${input.usernameDB}' );;" /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define( 'DB_PASSWORD', 'password_here' );%;" /"define( 'DB_PASSWORD', '${input.passwordDB}' );;" /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define( 'DB_HOST', 'localhost' );%;" /"define( 'DB_HOST', 'localhost' );;" / /var/www/html/mywordpresssite/wp-config.php
77      - sudo chown -R apache:apache
/var/www/html/mywordpresssite/
78      - sudo chmod -R g+w /var/www/html/mywordpresssite/
79      - sudo semanage fcontext -a -t httpd_sys_rw_content_t
"/var/www/html/mywordpresssite(/.*)?"
80      - sudo restorecon -R /var/www/html/mywordpresssite/
81      - systemctl enable httpd
82      - service httpd restart
83 attachedDisks:
84      - source: '${resource.Cloud_Volume_1.id}'
Cloud_Network_1:
85      type: Cloud.Network
86      properties:
87          networkType: existing
88          constraints:
89              - tag: 'subnet-cidr:10.50.0.0/24'
Cloud_Volume_1:
90      type: Cloud.Volume
91      properties:
92          capacityGb: 3
93
```



# 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, Multicast*
- CA** *Certificate Authority*
- CITIC** *Centro de Investigación en Tecnologías 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 Transceiver*

**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** [9]: 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** [10]: 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** : lugar 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** [11]: 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 dentro 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** [12]: 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** [13]: 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-Enterprise-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/installacion/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] VMware, “Multiple availability zones.” [En línea]. Disponible en: <https://docs.vmware.com/en/VMware-Cloud-Foundation/4.0/com.vmware.vcf.vxrail.admin.doc/GUID-0FA2DBCB-4522-46EC-B267-9F1B10FD9B26.html>
- [7] 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](https://docs.vmware.com/en/VMware-Cloud-Foundation/3.9/com.vmware.vcf.planprep.doc_39/GUID-202ECBCF-2CAA-4167-BA54-4EE1169D312C.html)
- [8] 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](https://www.vmware.com/resources/compatibility/vsan_profile.html?locale=en)
- [9] P. Traina, “Bgp-4 protocol analysis,” RFC 1774, DDN Network Information Center, Tech. Rep., 1995.

- [10] V. Infrastructure, “Resource management with vmware drs,” *VMware Whitepaper*, vol. 13, 2006.
- [11] E. Alliance and B. Kohl, “Ethernet jumbo frames,” 2009.
- [12] 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.
- [13] V. Törhönen, “Designing a software-defined datacenter,” 2013. [En línea]. Disponible en: <http://urn.fi/URN:NBN:fi:tty-201405261235>