



UNIVERSIDAD NACIONAL DE SAN JUAN

FACULTAD DE CIENCIAS EXACTAS FÍSICAS Y NATURALES
Departamento de Informática

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

**Migración de on-premise a un Data Center Virtual
Centralizado con Alta Disponibilidad**

TRABAJO FINAL

Autor

Oscar Damián Romero

Registro

13692

Asesor

Profesor Lic. Nelson Rodríguez

SAN JUAN

2026

RESUMEN

La gestión de los servidores implica toda la supervisión y el mantenimiento necesarios para que funcionen de forma fiable y a un nivel de rendimiento óptimo. Esto incluye gestionar el hardware, el software, la seguridad y las copias de seguridad para mantener el entorno informático operativo y eficiente. Este trabajo evalúa la importancia y las variadas actividades para la administración de servidores. Las buenas prácticas en la gestión de los recursos, permite un constante procesamiento de datos, brindando adecuadas herramientas de análisis de la información. Además, se centra en mantener una alta disponibilidad de servicios dirigido a los clientes, quienes requieren operar de manera ágil, simple y práctica, en cualquier momento del año. Es decir, mantener un servicio las 24 hs., los 365 días del año. Se analizará como la migración de arquitecturas de Data Centers convencionales a tecnologías de virtualización proporciona potentes herramientas que permiten enfrentar los nuevos desafíos empresariales.

ABSTRACT

Server management involves all the monitoring and maintenance necessary to ensure that servers operate reliably and at optimal performance levels. This includes managing hardware, software, security, and backups to keep the IT environment operational and efficient. This paper evaluates the importance and varied activities involved in server administration. Best practices in resource management enable constant data processing, providing adequate tools for information analysis. In addition, it focuses on maintaining high availability of services for customers who need to operate in an agile, simple, and practical manner at any time of the year. In other words, maintaining service 24 hours a day, 365 days a year. We will analyze how the migration from conventional data center architectures to virtualization technologies provides powerful tools that enable us to face new business challenges.

Palabras Claves

Virtualización, Data Center, Data Center migration, alta disponibilidad, balanceo de carga, hipervisor, máquinas virtuales, almacenamiento compartido.

Keywords

Virtualization, Data Center, Data Center Migration, High Availability, Load Balancing, Hypervisor, Virtual Machines, Shared Storage

INDICE

INDICE	2
AGRADECIMIENTOS	6
CAPÍTULO 1.....	7
Presentación y Descripción	7
1.1 Introducción	7
1.2 Antecedentes	8
1.3 Justificación	9
1.4 Objetivos.....	10
1.4.1 Objetivo General	10
1.4.2 Objetivos específicos	10
CAPÍTULO 2.....	11
Marco Teórico	11
2.1 Introducción	11
2.2 Virtualización	11
2.2.1 Tipos de virtualización.....	11
2.3 Hipervisor - Hypervisor	12
2.3.1 Tipos de hipervisores	12
2.4 VMWare	13
2.4.1 La historia de VMware.....	13
2.4.2 VMWare ESXi	14
2.4.2.1 Diferencia entre ESXi y ESX	14
2.4.2.2 Ventajas que ofrece ESXi.....	14
2.4.2.3 VMware y Linux	14
2.5 VMware vSphere	15
2.5.1 VMware vCenter Server	15
2.5.2 Componentes adicionales de VMware vSphere.....	15
2.5.3 Ventajas e inconvenientes de VMware vSphere.....	16
2.5.4 Puntos transversales que mejoraron versión a versión.....	16
CAPÍTULO 3.....	18
Inconvenientes de los Data Centers descentralizados	18
3.1 Introducción	18
3.2 Cambios de un Data Center en el tiempo.	18
3.3 Características de un Data Center virtual no centralizado.....	19
3.3.1 Distintos tipos de servidores físicos:.....	19
3.3.2 Variedad de Hypervisores:	19
3.3.3 Servers No Virtuales:	19
3.3.4 Gran diversidad VMs con recursos obsoletos:.....	19
3.3.5 Hosts sobrecargado:	19
3.3.6 Host con Hardware obsoleto.	20
3.3.7 Distintos tipos de conexión de red:	20

3.3.8 Información no realista de la estructura del Data Center	20
3.3.9 Limitada administración remota de los hosts físicos: Varios inconvenientes de.	20
3.4 Inconvenientes en la gestión en un Centro de Dato descentralizado	20
3.4.1 Gran complejidad en la administración de servidores independientes.	20
3.4.2 Aumento de downtime y discontinuidad del negocio	20
3.4.3 Inconvenientes para implementar nuevos sistemas y agregar nuevos servidores.	21
3.4.4 Problemas con el almacenamiento.	21
3.4.5 Inconvenientes para una buena política de seguridad y control.....	21
3.4.6 Inconveniente para aplicar actualizaciones.	22
3.4.7 Problema para implementar alertas y monitoreo y lograr una buena observabilidad.	22
3.4.8 Poca probabilidad de automatización de operaciones y mantenimiento.....	23
3.4.9 Problemas en las cargas de trabajo, saturación de algunos servidores.	23
3.4.10 Dificultad para implementar aislamientos de funcionalidad de servidores.	24
3.5 Visión global de un Data Center no centralizado	24
CAPÍTULO 4.....	25
Implementación de un Data Center Virtual Centralizado	25
4.1. Introducción	25
4.2 Infraestructura Física de un Data Center Virtual centralizado	25
4.2.1 Servidores físicos (Hosts ESXi).....	25
4.2.2 Almacenamiento / Datastores	26
4.2.2.1 Los principales tipos de almacenamiento compatibles	26
4.2.3 Red (Switching y Routing).....	26
4.3 Sistema de instalación.....	27
4.3.1 Controladoras de gestión de placas bases	27
4.3.2 Instalación de ESXi en un servidor	28
4.3.2.1 Configuración de BMC	28
4.3.2.2 Uso del visor de la consola virtual de iDRAC	28
4.3.3 Proceso de Instalación del ESXi	29
4.3.3.1 Instalación del primer host ESXi.....	29
4.3.3.2 Configuración básica del host ESXi.....	30
4.3.4 Despliegue de VMware vCenter Server Appliance (VCSA).....	32
4.3.4.1 Requisitos de sistema para la nueva instancia de vCenter Server Appliance	33
4.3.4.2 Requisitos de hardware para el dispositivo de vCenter Server	33
4.3.4.3 Requisitos de almacenamiento para el dispositivo de vCenter Server	34
4.3.4.4 Puertos necesarios en vCenter Server	34
4.3.4.5 Guía de instalación de VMware vCenter y prácticas recomendadas	35
4.3.4.5.1 Instalación y opciones de VMware vCenter	35
4.3.4.5.2 Instalación de VMware vCenter Appliance.....	35
4.3.4.5.2.1 Fase 1: Instalación de vCenter Server	37
4.3.4.5.2.2 Etapa 2: Configuración de vCenter Server.....	41
4.4 Crear Clusters de vSphere HA.....	43
4.4.1 Funcionamiento de vSphere HA	44
4.4.2 Hosts principales y secundarios en un cluster	44

4.4.3 vSphere Cluster Services.....	45
4.4.3.1 Máquinas virtuales del agente	45
4.4.4 Crear Datacenter.....	46
4.4.4.1 Nodos Suelos (Hosts Individuales)	46
4.4.4.2 Nodos en un Cluster (Cluster de Hosts)	46
4.4.4.3 Añadir un nodo a vCenter	47
4.4.4.3.1 Pasos Detallados	47
4.4.5 Creación de Cluster	48
4.5 Almacenamiento en vSphere vCenter	50
4.5.1 Datastores no compartidos	50
4.5.2 Datastores compartidos	50
4.5.3 Agregar un Datastore a vCenter	51
CAPÍTULO 5.....	53
Herramientas que potencian el uso de VMWare vSphere vCenter	53
5.1 Introducción	53
5.2 Herramientas Nativas de vCenter (Integradas en vSphere)	53
5.2.1 vMotion	53
5.2.1.1 Casos de uso de vMotion.....	53
5.2.1.2 Como funciona vMotion	54
5.2.2 Storage vMotion.....	55
5.2.2.1 Cómo Funciona (Paso a Paso).....	55
5.2.2.2 Beneficios Principales	55
5.2.3 DRS – Programador de Recursos Distribuidos	56
5.2.3.1 Cómo funciona DRS	56
5.2.4 High Availability (HA) – Alta Disponibilidad.....	56
5.2.4.1 Diferencia entre DRS y HA en VSphere.....	57
5.2.4.2 Requisitos del clúster VMware con HA	57
5.2.4.3 VMware vSphere HA proactiva	57
5.2.5 Fault Tolerance (FT):	57
5.2.5.1 Cómo funciona.	58
5.2.5.2 Diferencia con VMware HA (Alta Disponibilidad)	58
5.2.5.3 Limitaciones claves para decidir su uso	58
5.2.6 VMware Tools	59
5.2.6.1 Beneficios de instalar VMware Tools	59
5.2.7 vCenter Server.....	60
5.3 Herramientas de Gestión y Automatización Externas y/o Complementarias.....	60
5.3.1 PowerCLI	60
5.3.1.1 Ventajas de trabajar con PowerCli	61
5.3.2 RVTtools	61
5.3.2.1 Principales beneficios de usar RVTtools.....	62
5.3.3 vCenter Converter	63
5.3.3.1 Componentes de VMware vCenter Converter Standalone.....	63

5.3.3.2 Migración en frío y en caliente.....	63
5.3.4 MobaXterm/WinSCP	64
5.3.5 ESXCLI.....	64
5.3.5.1 Habilitar la consola ESXi Shell.....	64
5.3.6 vRealize Log Insight –VMware Area Operations for logs	64
5.3.6.1 Funcionamiento de vRealize Log Inight	65
5.3.6.2 Características principales de Log Insight.....	65
5.3.7 Herramientas de backup y replicación.	66
5.3.7.1 Principales soluciones de Backup y Replicación para VMware vCenter.....	66
5.3.7.2 Dispositivos físicos de respaldo de alto rendimiento	67
5.3.7.3 Ventajas y Desventajas de aplicar backup y replica.....	67
CAPÍTULO 6.....	68
Mejoras en la administración de DataCenter, usando VMWare vCenter como Management principal.....	68
6.1 Introducción	68
6.2 Migración al nuevo de Data Center – Análisis y planificación para la migración	68
6.2.1 Priorización.	68
6.2.2 Depuración de tecnología obsoleta y sistemas no utilizables	69
6.2.3 Agrupamiento de Sistemas por características y funcionalidades comunes.	69
6.2.4 Inconvenientes para mantener la disponibilidad durante la migración	70
6.3 Ventajas de administrar un Data Center virtualizado y centralizado.....	70
6.3.1. Mantener distintos ambientes independientes.....	70
6.3.2 Ambiente de prueba idóneo.	71
6.3.3 Herramienta para clonar VMs a diferentes clusters.	71
6.3.4 Snapshots –agilizar nuevas implementaciones.	72
6.3.5 Mayor disponibilidad de recursos	72
6.3.6 Facilidad para actualizar versiones y parchado de SO.....	73
6.3.7 Estructura física que acompañe los cambios del negocio.	73
6.3.8 Facilidad para evolucionar la infraestructura de hardware.	74
6.3.9 Plantillas para agilizar la creación de nuevos servers	74
6.3.10 Actividades para mantener la performance del Data Center.....	75
6.3.11 Optimizar el almacenamiento. Distintos tipos de Aprovisionamiento.....	76
6.3.12 Herramientas de Backup y Recovery	76
6.3.13 Fácil visualización de alertas de hardware.....	77
6.4 Características indispensables de un Data Center	78
6.4.1 Buena escalabilidad.....	78
6.4.2 Alta Disponibilidad (HA).....	79
6.4.3 Facilidad para implementar actividades proactivas	79
6.4.3.1 vRealize Operations	80
CONCLUSIONES.....	81
BIBLIOGRAFIA.....	83

AGRADECIMIENTOS

A la Facultad de Ciencias Exactas, Físicas y Naturales, a sus profesores y compañeros, con quienes durante mi paso como estudiante no solo adquirí conocimientos, sino también valores como la solidaridad, la inclusión, el compromiso y el pensamiento crítico; y lo más importante, conocí a mis grandes amigos.

A mi familia, que siempre me acompañó y sostuvo en cada etapa de este camino.

A mi asesor de tesis, Prof. Nelson Rodríguez, quien no solo mostró una gran predisposición durante la realización de este trabajo, sino que fue el gran impulsor para que pudiera dar este importante paso.

Y por último, **a las personas más importantes de mi vida, a mi mamá**, que desde su lugar siempre me acompañó e inspiró, y **a mi papá**, quien, a pesar de su ausencia, sigue presente en cada paso de mi vida. Este logro también es de ustedes.

CAPÍTULO 1

Presentación y Descripción

1.1 Introducción

En estos nuevos tiempos, donde rige la inmediatez como principal filosofía de mercado, muchas empresas enfrentan constantes operaciones críticas que no pueden permitirse interrupciones. Son empresas que dependen del acceso instantáneo de datos, transacciones y aplicaciones para operar 24/07. Estas empresas invierten en infraestructura con redundancia (servidores, redes, energía) y diseño activo-activo para asegurar que sus sistemas no fallen, garantizando continuidad operativa y máxima fiabilidad

Algunos sectores que Requieren Alta Disponibilidad:

- **Sector Financiero:** Manejo de transacciones sensibles y procesamiento de datos en tiempo real (Bancos, Bolsas de Valores, Billeteras Virtuales).
- **Salud:** Acceso inmediato a historiales médicos, resultados de exámenes y aplicaciones críticas (Hospitales, Telemedicina).
- **Servicios de Emergencia y Gobierno:** Coordinación, seguimiento y comunicación instantánea (Policía, Bomberos, Servicios Públicos).
- **Tecnología y Telecomunicaciones:** Proveedores de servicios en la nube, plataformas de hosting, redes (Google, Microsoft, Amazon, AT&T).
- **Comercio Electrónico (E-commerce):** Gestión de inventarios, transacciones y atención al cliente sin interrupciones (Amazon, etc.).
- **Manufactura y Logística:** Control de procesos críticos en línea, seguimiento en tiempo real de producción y cadena de suministro.
- **Medios y Entretenimiento:** Streaming de contenido y plataformas que requieren disponibilidad constante.

Estos cambios de reglas, trajo aparejado un constante aumento de análisis y procesamiento de información. Las modificaciones e implementaciones de nuevos sistemas paso a ser moneda corriente. Soportar estos cambios constantes, significó un crecimiento exponencial en la infraestructura de TI.

Los servidores virtuales han resultado una solución eficiente que permite alojar varios servidores dentro de un servidor físico, permitiendo algunas ventajas como aumento de disponibilidad, optimización de recursos, ahorro de dinero, provisión rápida de servidores y mayor eficiencia y recuperación, entre otras. Si bien la virtualización en el Cloud resulta ventajosa, dado que toda la gestión de los servidores es llevada a cabo por la empresa proveedora de servicios Cloud, en varias instituciones, por numerosas razones, los servidores deben ser propietarios de la entidad y por lo tanto administrados por profesionales o técnicos de la misma.

Muchas empresas comienzan con un Centros de Cómputos que en principio cumple los requerimientos necesarios. No se le daba la importancia necesaria de implementar una buena política de Administración de TI que soporte fácil escalabilidad y alta disponibilidad. Estos Centro de Cómputos generalmente estaban formados por un conjunto de varios servidores físicos, de distintos modelos, marcas y topologías. Si bien, muchos contaban con estructura de

virtualización, administrarlos resultaba complicado, poco intuitivo, y difícil de mantener. Al tratarse de empresas que, por su tipo de actividad, aumentaban no solo la disponibilidad de sus servicios, sino también la capacidad de procesamiento, dejaron de enfrentar un crecimiento temporal. El crecimiento de su infraestructura paso a ser constante y muy dinámico, dificultando una adecuada planificación. La inversión en los Centros de Cómputos muchas veces se limitaba en adquirir recursos con nuevas tecnologías que ampliaran su capacidad, pero la mayoría de las veces conviviendo con lo que ya estaba implementado. La administración para dar un buen servicio de TI, se volvía insostenible

Esto provocó la necesidad de realizar un cambio radical en la infraestructura. No solo a algo más homogéneo, sino también más robusto, más rápido, que permitiera una buena escalabilidad y cuya administración resultara más simple. Una decisión a nivel jerárquico, que tome como principal eje, un cambio de paradigma en el Data Center.

Para llevar a cabo estos nuevos cambios, se debe adquirir nuevas tecnologías de hardware y software para la migración del Data Center. Con el uso de software VMWare, servidores de alto rendimiento, datastores y switch de alta velocidad, se logra una administración simplificada y centralizada de todos los recursos. Además permite crecimiento físico escalable; recuperación instantánea de sistemas; facilita las nuevas implementaciones; optimiza el procesamiento y almacenamiento; utiliza redundancia para una alta disponibilidad de servicios; y facilita un real monitoreo de la performance.

1.2 Antecedentes

Históricamente, entre la década de los 80 y 90, los data centers se construyeron bajo un modelo basado en servidores físicos dedicados, donde cada aplicación o servicio se ejecutaba sobre un servidor independiente. Con gran desperdicio de hardware, con un uso entre un 10 y 20% de su capacidad. Estos entornos estaban formados por hardware heterogéneo, adquirido en distintos momentos, con diferentes capacidades, arquitecturas y sistemas operativos.

A mediados de los 90 con la llegada de Internet Comercial, generó un gran impacto en los Data Centers. Con la popularización de la World Wide Web las empresas comienzan a incorporar sitios web corporativos, servidores de correo accesibles desde internet, servidores web (HTTP), servidores DNS, Firewall y aparece el concepto de DMZ. Los Data Center empiezan a estar expuesto al exterior, con mayor dependencia de conectividad

En los años 2000 se instaura a Internet como pilar del negocio. Hay una gran explosión del e-commerce, banca online y sistemas web. Las aplicaciones empresariales migran a modelos web. Internet deja de ser “un extra” y pasa a ser crítico.

Esta gran influencia de internet provocó un crecimiento acelerado y desorganizado de la infraestructura, conocido comúnmente como “server sprawl”. Cada nueva necesidad implicaba la incorporación de un nuevo servidor físico, incrementando la complejidad del entorno. La falta de estandarización en hardware, software y configuraciones dificultaba una administración eficiente del Data Center. Comenzaron a aparecer nuevas necesidades como alta disponibilidad, redundancia de enlaces. Los Data Center pasaron a ser más complejos y costosos. Los grandes problemas que tuvieron que enfrentar fue la escalabilidad, el downtime y la administración manual.

Ante estas problemáticas, que tuvo sus comienzos en los 90, surgió la virtualización de servidores como una alternativa tecnológica que permitió desacoplar los servicios del hardware físico. Plataformas desarrolladas por empresas como VMware, que impulsaron estos cambios,

introdujeron la posibilidad de consolidar múltiples servidores virtuales sobre un mismo host físico, mejorando el uso de los recursos. Si bien la virtualización presentó grandes mejoras, no soluciona los grandes desafíos que comenzaron a tener la mayoría de las empresas, como una adecuada administración de sus recursos, mantener la disponibilidad de sus servicios 24x7 y lograr una adaptabilidad a los cambios continuos. Sin embargo, esta evolución sentó las bases a un nuevo paradigma de Data Center.

Debido al auge de internet, ya a finales de los 90 y a comienzos de los 2000, surge la necesidad de una gestión centralizada en los Data Centers. Pero recién se materializa entre 2004 y 2008, y se consolida a partir de 2010. Aparecieron nuevos conceptos como la virtualización masiva, la introducción de clusters con automatización de alta disponibilidad, balanceo de carga y mantenimiento sin downtime.

VMware vSphere vCenter como herramienta de administración centralizada, respondió adecuadamente a esas necesidades. Unificó la gestión viendo a toda la infraestructura como un todo, permitió automatizar tareas operativas, mejoró la disponibilidad y continuidad del negocio, facilitó el crecimiento y la escalabilidad del data center

La necesidad de gestión centralizada de los Data Center surge como respuesta al crecimiento exponencial de servidores, la criticidad de los servicios expuestos a Internet y la demanda de alta disponibilidad y continuidad del negocio, problemas que no podían resolverse mediante la administración aislada de servidores físicos.

1.3 Justificación

La migración de un Data Center compuesto por servidores heterogéneos administrados de manera individual a uno totalmente virtual, organizado en clusters y gestionado centralizadamente mediante VMware vCenter Server, se justifica por la necesidad de mejorar la eficiencia operativa y la disponibilidad de los servicios de TI, asegurando la continuidad del negocio, alineando la infraestructura tecnológica para ser adaptable a las demandas actuales de un entorno tan cambiante.

En un Data Center tradicional no centralizado, la administración independiente de cada servidor es manual y aislada, generando altos niveles de complejidad y propensa a errores humanos. Con dificultades para estandarizar configuraciones y tiempos prolongados de indisponibilidad ante fallas o tareas de mantenimiento, la recuperación es muy dependiente del hardware, generando altas probabilidades de downtime. Además, la heterogeneidad del hardware suele provocar un uso ineficiente de los recursos, con servidores subutilizados y otros sobrecargados. Con escalabilidad demasiado limitada y muy costosa. Estas limitaciones afectan directamente la disponibilidad de los servicios, el rendimiento de las aplicaciones y la capacidad de crecimiento del negocio.

La creciente demanda hace necesario adoptar un modelo de infraestructura más dinámico, resiliente y eficiente, donde los recursos puedan asignarse y gestionarse de forma centralizada. La virtualización permite abstraer el hardware físico, consolidar múltiples cargas de trabajo en menos servidores y aprovechar mejor los recursos (CPU, memoria y almacenamiento) reduciendo considerablemente el costo. Al implementar clusters, se habilitan mecanismos de alta disponibilidad, balanceo de carga y recuperación automática ante fallas gracias a la migración en caliente, reduciendo significativamente el downtime y el impacto de incidentes en la operación del negocio, además de brindar mayores características de flexibilidad y escalabilidad.

Por otro lado, la adopción de un Data Center virtual con administración centralizada mediante vCenter posibilita una gestión unificada y proactiva del entorno, facilitando el monitoreo, la automatización de tareas operativas, la aplicación de políticas comunes y la planificación del crecimiento futuro. Multiplica la ejecución de una gran diversidad de máquinas virtuales de forma aislada y segura, consolidadas en menos hosts. Esto no solo optimiza los tiempos de administración, sino que también reduce los tiempos de inactividad ante fallas de hardware, mejora la seguridad, la trazabilidad y la capacidad de respuesta ante cambios o incidentes. También facilita implementaciones de backups, replicación y recuperación ante desastres.

En este contexto, la migración no responde únicamente a una modernización tecnológica, sino también a ofrecer una infraestructura que garantice una mayor estabilidad, flexibilidad y sostenibilidad operativa, adaptándose a las necesidades actuales y futuras del negocio, superando ampliamente las limitaciones del modelo tradicional

1.4 Objetivos

1.4.1 Objetivo General

Analizar la migración de un Data Center tradicional, compuesto por varios servidores heterogéneos administrados de manera independiente, hacia un Data Center totalmente virtual con gestión centralizada con vSphere vCenter.

1.4.2 Objetivos específicos

- Describir la arquitectura de un Data Center tradicional no centralizado y sus principales limitaciones.
- Analizar el funcionamiento de la virtualización con VMware vSphere y la administración centralizada mediante VMware vCenter Server.
- Analizar el rol de los clusters en la distribución de recursos, alta disponibilidad y balanceo de carga.
- Identificar los componentes necesarios para implementar el nuevo data center, como hosts ESXi, almacenamiento compartido, redes virtuales, etc.
- Evaluar las mejoras en la administración y monitoreo de servidores al pasar de una gestión individual a una centralizada.
- Analizar el impacto en la continuidad del negocio, reduciendo los tiempos de inactividad (downtime) mediante funciones como High Availability (HA) y vMotion.
- Comparar los procesos de mantenimiento antes y después de la migración (actualizaciones, ampliaciones, recuperación ante fallos, etc).
- Determinar los beneficios en escalabilidad y optimización de recursos que ofrece un entorno virtualizado y centralizado.

CAPÍTULO 2

Marco Teórico

2.1 Introducción

Toda empresa que necesita contar con una infraestructura de sistemas muy grande y compleja, opta por el uso de virtualización. Los servidores virtuales han resultado una solución eficiente que permite alojar varios servidores dentro de un servidor físico, permitiendo algunas ventajas como aumento de disponibilidad, optimización de recursos, ahorro de dinero, provisión rápida de servidores y mayor eficiencia y recuperación, entre otras.

Si bien actualmente no se concibe la idea de no usar virtualización en las estructuras de TI, en muchos casos es necesario contar con servicios adicionales como por ejemplo una alta disponibilidad en sus servicios. En este capítulo se tratarán los conceptos que son considerados elementales, para una mejor comprensión de este trabajo final.

2.2 Virtualización

La virtualización es una tecnología que permite crear varios entornos simulados o recursos específicos desde un solo sistema de hardware físico. Gracias al hipervisor, un software que se conecta directamente al hardware, se puede dividir un sistema en entornos separados y distintos, conocidos como máquinas virtuales. Estas máquinas virtuales dependen de la capacidad del hipervisor de separar los recursos de la máquina del hardware y distribuirlos adecuadamente [1].

La virtualización permite utilizar el hardware de forma más eficiente y ofrece un mayor retorno de inversión del hardware de una empresa. Hoy en día, la virtualización es una práctica estándar en la arquitectura de TI

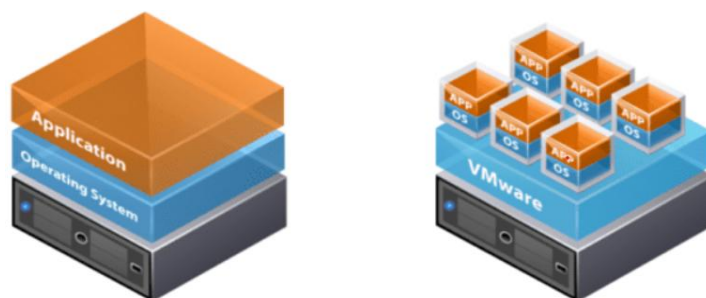


Figura 1. Arquitectura tradicional Vs. Arquitectura virtual. Recuperada de (Atalanta, 2022)

2.2.1 Tipos de virtualización

Los principales tipos de virtualización son

- **Virtualización de servidores:** Crea servidores virtuales (VMs) para ejecutar múltiples sistemas operativos y aplicaciones en un único servidor físico. Esto optimiza el uso del hardware y reduce costos.
- **Virtualización de almacenamiento:** Combina múltiples dispositivos de almacenamiento físico (discos duros, SSD) en un único "pool" de almacenamiento que se administra como un solo recurso.

- **Virtualización de red:** Permite dividir una red física en múltiples redes lógicas o combinar varias redes físicas en una sola, gestionada a través de software. Ejemplos comunes son las VLANs y la SDN (Redes Definidas por Software).
- **Virtualización de escritorio (VDI):** Permite a los usuarios acceder a un escritorio y a sus aplicaciones desde cualquier lugar y dispositivo. El sistema operativo y los datos residen en un servidor centralizado.
- **Virtualización de aplicaciones:** Ejecuta aplicaciones en un entorno virtual aislado del sistema operativo, lo que evita conflictos de configuración y facilita la distribución y gestión.

2.3 Hipervisor - Hypervisor

Un hipervisor, también conocido como monitor de máquina virtual o VMM, es un software que crea y ejecuta máquinas virtuales (VM). Un hipervisor permite que un servidor anfitrión admita múltiples máquinas virtuales invitadas mediante el uso compartido virtual de sus recursos, como la memoria y el procesamiento.

Los hipervisores permiten aprovechar mejor los recursos disponibles del sistema y proporcionan mayor movilidad de TI, ya que las máquinas virtuales invitadas son independientes del hardware del host. Esto significa que se pueden trasladar fácilmente entre diferentes servidores. Dado que varias máquinas virtuales pueden ejecutarse en un solo servidor físico con un hipervisor, este reduce: Espacio, Energía y Requisitos de mantenimiento

Los hipervisores hacen posible la virtualización al traducir las solicitudes entre los recursos físicos y virtuales. En ocasiones, los hipervisores de hardware integrado se encuentran integrados en el firmware al mismo nivel que el sistema básico de entrada/salida (BIOS) de la placa base para permitir que el sistema operativo del host acceda al software de virtualización y lo utilice.

2.3.1 Tipos de hipervisores

Existen dos tipos de hipervisores que pueden usarse para la virtualización.

- **Tipo 1 – Bare metal:** Este tipo de hipervisor, también conocido como el original o de servidor dedicado, se ejecuta directamente en el hardware del host para gestionar los sistemas operativos guests. Funciona como un SO host y programa los recursos de las máquinas virtuales directamente en el hardware. Suele usarse en los centros de datos empresariales o en otros entornos que se basan en servidores. Algunos ejemplos son Microsoft Hyper-V, VMware ESXi, KVM (Kernel-based Virtual Machine), Citrix Hypervisor, etc.

- **Tipo 2:** Estos hipervisores también se conoce como hipervisor alojado y se ejecuta en un sistema operativo convencional como una capa del software o una aplicación. Funciona extrayendo los sistemas operativos guest del sistema operativo host. Los recursos de la máquina virtual se programan en un sistema operativo host, que después se ejecuta en el sistema de hardware. Estos hipervisores son ideales para los usuarios individuales que desean ejecutar varios SO en una computadora personal. VMware Workstation y Oracle VirtualBox son ejemplos de este tipo de hipervisores [2].

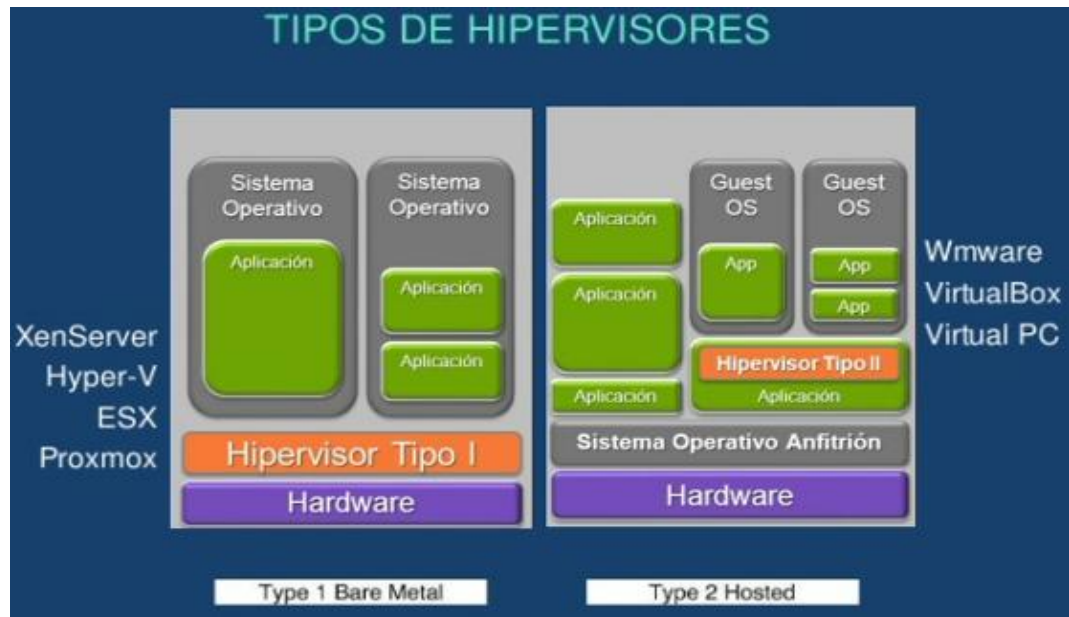


Figura 2. Arquitectura de los tipos de hipervisores. Recuperado de (Valenhaus 2025)



Figura 3. Tipos de Hipervisores. Recuperado de (Francisco Javier Cruces Doval, 2025)

2.4 VMWare

VMware desarrolla productos de software de virtualización que son cruciales para las infraestructuras de tecnología de la información de muchas empresas. Cuando se habla de infraestructura de TI, se refiere a los componentes de hardware, software y red en los que las empresas confían para gestionar y ejecutar sus entornos de TI de manera eficaz [3].

La virtualización permite un uso más eficiente del hardware informático y un mayor retorno de la inversión en hardware de una organización. También permite a los proveedores de la nube, por ejemplo, Amazon Web Services (AWS), IBM Cloud, Microsoft Azure y Google Cloud, atender a más usuarios con su hardware informático físico existente.

2.4.1 La historia de VMware

En 1998, un equipo de científicos (Diane Greene, Scott Devine, Mendel Rosenblum, Edward Wang y Edouard Bugnion) fundó VMware. En 1999, la empresa con sede en Palo Alto comenzó VMware Workstation 1.0, el primer producto comercial que permitía a los usuarios ejecutar múltiples sistemas operativos como máquinas virtuales en una sola PC.

VMware entró en el mercado de servidores en 2001 con VMware GSX Server (alojado) y VMware ESX Server (sin host). En 2004, EMC Corporation adquirió VMware. En 2016, Dell Technologies adquirió EMC y absorbió VMware. VMware creció hasta convertirse en el

principal proveedor de servicios de virtualización con vSphere, su plataforma de virtualización de servidores, que mantuvo el número de cuota de mercado con más de 500 000 clientes.

En diciembre de 2023, la empresa de semiconductores Broadcom completó su adquisición de VMware por 69 mil millones de dólares con el objetivo de expandir su estrategia multinube. Broadcom ha rebautizado la empresa como VMware by Broadcom. Para simplificar, nos referiremos a ella como VMware

Desde la adquisición, Broadcom ha consolidado su oferta de productos en dos paquetes principales: VMware Cloud Foundation (VCF) y VMware vSphere Foundation (VVF). Además, Broadcom ha hecho la transición de VMware de las licencias perpetuas y las renovaciones de soporte y suscripción a un modelo de precios basado en suscripciones [4].

2.4.2 VMWare ESXi

ESXi de VMware es un hipervisor de tipo 1 o coloquialmente **bare-metal** que se ejecuta directamente en un servidor físico instalado y se puede utilizar sea cual sea el sistema operativo. El software vSphere se utiliza para la administración. ESXi se basa en el vmkernel y prescinde de su propio sistema operativo de consola, lo que significa que el hipervisor requiere mucho menos espacio de almacenamiento que otras opciones. VMware introdujo por primera vez ESXi en 2001 y todavía lo ofrece en la actualidad. ESXi significa “Elastic Sky X integrated” [5].

2.4.2.1 Diferencia entre ESXi y ESX

ESX también es un hipervisor de tipo 1 y, al igual que su sucesor ESXi, proviene de VMware. A diferencia de la versión más reciente, ESX tiene su propio sistema operativo de consola. Esto significa que el hipervisor requiere mucho más espacio de almacenamiento. Desde la versión 5.0 de vSphere, solo se utiliza ESXi, ya que la variante más ligera ofrece claras ventajas en cuanto a la instalación y la memoria necesaria.

2.4.2.2 Ventajas que ofrece ESXi

ESXi ofrece numerosas ventajas, sobre todo en comparación con su predecesor ESX, que requiere mucho más espacio de almacenamiento. Se pueden ahorrar costes, consumo y espacio cuando se virtualizan centros de datos completos. Sin embargo, la seguridad contra fallos se mantiene, por lo que no surgen desventajas relevantes en este campo. Gracias a su proximidad al hardware, ESXi ofrece un gran rendimiento y aprovecha al máximo los recursos disponibles. La gestión se centraliza a través del hipervisor y los sistemas virtualizados pueden exportarse fácilmente. También a su favor se encuentra la gran flexibilidad y la rapidez de instalación. Si se utiliza ESXi en servidores alquilados, también se reducen los costes. Además, existen las opciones de escalado mencionadas anteriormente [6].

2.4.2.3 VMware y Linux

VMware confió en Linux durante sus primeros años de historia. La primera versión de su hipervisor, ESX, incluía un kernel de Linux (la parte central de un sistema operativo que administra el hardware de la computadora). Cuando VMware lanzó ESXi, reemplazó el kernel de Linux por el suyo propio. ESXi es compatible con varios sistemas operativos invitados de Linux, incluidos Ubuntu, Debian y FreeBSD.

2.5 VMware vSphere

VMware vSphere® aprovecha la potencia de la virtualización para transformar los centros de datos en infraestructuras de computación en la nube simplificadas, lo que permite que las organizaciones de TI ofrezcan servicios de TI flexibles y confiables.

Los dos componentes principales de vSphere son VMware ESXi™ y VMware vCenter Server®. Los componentes adicionales de vSphere están disponibles como complementos que extienden la funcionalidad del producto vSphere [7].

2.5.1 VMware vCenter Server

vCenter Server es la plataforma de gestión centralizada de VMware para entornos virtuales vSphere, permitiendo a los administradores controlar múltiples servidores físicos (hosts ESXi) y sus máquinas virtuales (VMs) desde una única consola web, facilitando tareas como aprovisionamiento, migración en vivo (vMotion), monitorización, automatización y gestión de recursos y usuarios. Actúa como el "panel de control" que unifica y simplifica la administración de toda la infraestructura virtualizada, ofreciendo funciones avanzadas como alta disponibilidad y gestión de clústeres.

2.5.2 Componentes adicionales de VMware vSphere

Aunque vSphere es un conjunto de componentes de software, su implementación requiere tanto la infraestructura de software como la física necesaria para alojar y administrar los entornos virtuales. La topología física incluye los siguientes componentes:

- Servidores x86 estándar para alojar las máquinas virtuales y el software de gestión.
- Infraestructura de almacenamiento, como sistemas de almacenamiento conectados a la red o redes de área de almacenamiento (SAN).
- Red IP y adaptadores físicos para facilitar las comunicaciones.
- Dispositivos para alojar los clientes de gestión.

Aunque ESXi y vCenter Server son fundamentales para la plataforma vSphere, otros componentes de software también desempeñan funciones importantes en su funcionamiento. Por ejemplo, un agente de vCenter Server se ejecuta en cada host administrado, recopilando información para vCenter Server y ejecutando las operaciones comunicadas desde el servidor. También existe un agente que permite a los clientes de vSphere interactuar directamente con los hosts ESXi.

Otros componentes incluyen tc Server, que admite los servicios web de vCenter, y la base de datos de vCenter, que mantiene el estado de cada máquina virtual, host y usuario. El servidor también dispone de varios complementos para proporcionar características y funcionalidades adicionales. Además, vSphere instala un servicio de inicio de sesión único (SSO – Single Sign-On) que incluye diversos componentes propios, como un servidor de administración, el Servicio de tokens de seguridad, el Servicio de directorio de VMware y el Servicio de búsqueda de vCenter.

Otro aspecto importante para una implementación de vSphere es el conjunto de interfaces de cliente disponibles para administrar el entorno y sus componentes. La plataforma ofrece tres tipos de interfaces de cliente:

- **Cliente vSphere.** Un cliente web basado en Hypertext Markup Language 5 que sirve como interfaz principal para conectarse y administrar instancias de vCenter.

- **Ciente de host de VMware.** Un cliente basado en web para administrar hosts ESXi que no están conectados a una instancia de vCenter Server.
- **Interfaces de línea de comandos de vSphere.** Varias interfaces disponibles para configurar máquinas virtuales, hosts ESXi e instancias de vCenter Server.

La plataforma vSphere también proporciona **vSphere Cluster Services (vCLS)**, que se ejecuta en todos los clústeres de vSphere. Esta solución utiliza máquinas virtuales de agente para mantener el buen funcionamiento de los servicios del clúster y garantizar que este pueda seguir operando si vCenter Server deja de estar disponible. Además, supervisa los recursos que consumen las máquinas virtuales de vCLS y los protege contra la eliminación accidental [8].

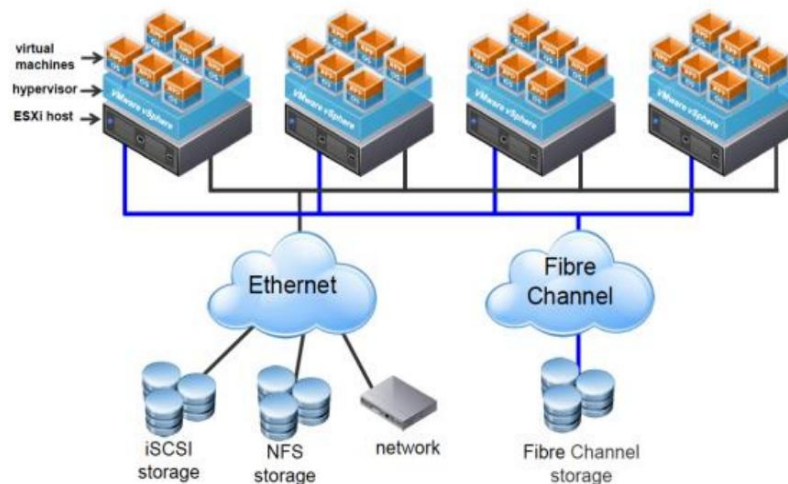


Figura 4. Estructura física de una arquitectura virtual. Recuperada de (Universidad Carlos III de Madrid, 2016)

2.5.3 Ventajas e inconvenientes de VMware vSphere

Como ocurre con cualquier plataforma de software, también tiene sus ventajas e inconvenientes.

La **principal ventaja** de la plataforma radica en su tecnología probada. Además, es estable y fiable. Asimismo, admite clústeres de alta disponibilidad e incluye diversas funciones para simplificar las implementaciones de máquinas virtuales. Gracias a la amplia implementación de VMware y a su gran base de usuarios, los administradores pueden acceder a una gran cantidad de información, como ayuda en línea, artículos técnicos, foros de usuarios, vídeos y mucho más.

Quizás la **mayor desventaja** de vSphere sea su complejidad. Con el paso de los años, los administradores han expresado su preocupación por la usabilidad y la dificultad del producto. Además, la complejidad de la plataforma puede dificultar la resolución de problemas. La plataforma también ha tenido fama de ser costosa debido a su sistema de licencias excesivamente complejo [8].

2.5.4 Puntos transversales que mejoraron versión a versión

Cada versión y actualización de vCenter busca ser más rápida, segura, escalable y fácil de usar, adaptándose a las nuevas demandas de la virtualización y la nube. Los puntos más notorios son los siguientes:

Administración centralizada: el VCSA y el cliente HTML5 crearon una experiencia de administración más estable y centralizada (mejor UI, API y automatización).

Escalabilidad y límites: cada generación elevó límites (más vCPUs, RAM por VM, hosts por cluster) y optimizó desempeño para infra a escala.

Seguridad: cifrado de VM, Secure Boot, mejoras en control de acceso y hardening del appliance fueron prioridad desde 6.x.

Almacenamiento y redes: mejoras en VASA/vVols, integración con vSAN, y en 8.x el offload a DPUs para funciones de red/seguridad.

Soporte para workloads modernos: desde vSphere 7 la plataforma integra Kubernetes (Tanzu) y en vSphere 8 se reforzó soporte para GPU/AI y arquitecturas DPU.

Lifecycle / mantenimiento: vLCM y mejoras en updates/patching (incluyendo live patch en Updates de v8) reducen downtime operativo.

CAPÍTULO 3

Inconvenientes de los Data Centers descentralizados

3.1 Introducción

Este capítulo abordará la descripción de un Data Center tradicional, con combinación de servers físicos dedicados e implementaciones virtuales. Tener presente que se trata de un Data Center con muchos años de funcionamiento y con constante incorporación de nuevas tecnologías, provocando la convivencia de una diversidad de hardware y software, varios ya obsoletos. Todo muy segmentado y con dificultad para ejecutar buenas prácticas para su administración. Sin herramientas para una administración centralizada. Estas características producen alto downtime y escalabilidad muy limitada, principales problemas a solucionar en un Data Center de este tipo.

3.2 Cambios de un Data Center en el tiempo.

Para entender el motivo del porque se llega a un Data Center con gran variedad de hardware y software, todo disociado y con gran dificultad para administrarlo, es importante entender la incorporación constante de nuevas tecnologías, nuevas versiones y que no siempre era posible migrar todo. Siguiendo este contexto, la incorporación de nuevas tecnologías no solo estaba motivado para mejorar la performance de los sistemas existentes, sino también para soportar nuevas implementaciones de sistemas de herramientas y servicios del negocio.

Como se mencionó, no siempre era posible migrar todo a las nuevas tecnologías, sino que se priorizaba migrar las más importantes o se destinaba para implementar nuevos sistemas. Esto provocó que convivieran lo nuevo con lo ya instalado. Con el paso del tiempo y sumado al crecimiento constante de nuevos sistemas para mejorar los servicios del negocio, fomentaba la situación de dejar varios sistemas funcionando en estructuras obsoletas

En un comienzo eran servidores físicos dedicados, una aplicación asociada a un servidor. La administración era manual y local. Muy baja estandarización de hardware y software. La escalabilidad muy escasa, limitada a la compra e instalación de nuevos servidores. El costo era muy elevado.

A medida que pasaba el tiempo se incorporaban servidores más potentes, con redundancia física, y conexiones de red con mayor performance. También se comenzaron a organizar físicamente en racks, con KVMs para administrar todos los de un mismo rack. Se comenzaron a usar algunos criterios para agruparlos físicamente.

En años más recientes se incorporaron servers con tecnologías de virtualización (VMware, Hyper-V, Xen). Donde múltiples VMs estaban en un mismo host físico. Aprovechando más los recursos y bajando el costo. Disminuyendo la cantidad de server físicos a administrar.

Todo este contexto posibilita entender los motivos por el que un Data Center con contante crecimiento, esté formado por tecnologías tan diversas y cuya administración era muy costosa sin lograr resultados eficientes. Donde cualquier inconveniente generaba alto downtime, afectando directamente a funcionalidad de la organización.

Esto empujó a encarar un cambio radical, con la incorporación de nuevas tecnologías que permitían una administración integral muy diferente a la actual.

3.3 Características de un Data Center virtual no centralizado

Características más importantes de un Data Center que creció sin un buen planeamiento.

3.3.1 Distintos tipos de servidores físicos: Se contaban con muchas marcas y modelos de servidores, la mayoría con plataformas de virtualización, pero con un porcentaje importante de servers dedicados. Había servidores IBM, Dell PowerEdge 850, 910, 920., HP, etc. También diferían en su formato físico, si bien la mayoría eran servers rack, algunos también del tipo tower y blade.

3.3.2 Variedad de Hypervisores: La virtualización es una herramienta que ya se usa bastante en soluciones empresariales. Por lo que es muy común encontrar muchas virtualizaciones implementadas. El problema es la gran variedad de esos hipervisores, tanto en marcas, como en versiones. En su mayoría Hyper-V, ESX y ESXi. Esta gran diversidad no permitía una mínima integración para mejorar la administración.

3.3.3 Servers No Virtuales: Como hablamos de Data Centers que llevan gran cantidad de años. Es muy común encontrarse con varios servers que no estaban virtualizados, sino funcionando directamente en un host dedicado. No solo eran servers físicos muy obsoletos, también con sistemas operativos obsoletos. Además, para aprovechar en su momento los recursos, se colocaban varios servicios o sistemas conviviendo en esa misma estructura que no estaban relacionados. Si algún sistema de un server tenía inconvenientes, era muy difícil ocuparse de manera aislada sin afectar a los demás servicios que convivían en el mismo server.

3.3.4 Gran diversidad VMs con recursos obsoletos: Esta gran diversidad no solo estaba en la arquitectura física y los hipervisores, sino también en la gran variedad de máquinas virtuales. Muchas VMs con sistema operativo obsoleto, y la mayoría una vez creada, se le hacía un mantenimiento escaso. Solo si presentaba inconvenientes. Salvo en casos muy necesarios, se les aplicaba parches del SO, y en el menor de los casos se migraban a versiones de SO más actuales. Si bien eran muy pocas, pero habían VMs con Windows NT o Windows server 2000. Tener en cuenta que trabajar con estos servers, significaba tiempo de no tener disponible el sistema.

3.3.5 Hosts sobrecargado: Se trata de **host dedicados** (sin tecnología de virtualización), con varios sistemas funcionando en un mismo sistema operativo sin criterio para agruparlos. Algunos sistemas crecieron mucho más de lo previsto, sumado a que convivían con otros servicios que en varios casos eran considerados críticos. Los recursos como almacenamiento, CPU, memoria y en varios casos la elevada tasa en la red generaba importantes sobrecargas. Servicios que estaban funcionando bien se veían afectados por otros servicios dentro del mismo servidor que tenían muchos inconvenientes.

Una problemática muy similar también se producía en **host con virtualización**. En un comienzo se implementaban VMs con un buen grado de rendimiento, acorde al hardware subyacente, funcionando de manera holgada. Pero con el pasar del tiempo los sistemas de varias VMs crecían y por ende consumían más recursos de los previstos, provocando que el host físico se saturara constantemente. Una o dos VMs sobrecargadas, afectaban el funcionamiento del resto de las VMs.

3.3.6 Host con Hardware obsoleto. Estos servidores presentaban constantes inconvenientes. Alertas de degradación, discos que dejaban de funcionar y se reemplazaban por otros discos viejos y que estaban en desuso, problemas con el power, placas de red, etc. Si bien se los priorizaba para migrar, pero que siguieran activos era producto del alto costo para migrarlos, sobre todo por el tiempo de disponibilidad. Tener en cuenta que migrar sistemas o VMs para que funcione sobre estructuras con varios cambios tecnológicos significativos, implica grandes cambios para adaptar al sistema, por no decir una reprogramación del mismo.

3.3.7 Distintos tipos de conexión de red: Las conexiones de red no eran heterogéneas, ya sea en tecnologías, velocidades, topologías o fabricantes; provocando varios inconvenientes en rendimiento y estabilidad. Se tornaba muy complejo gestionarla, con alta probabilidad de cometer errores humanos. Situación que propiciaba los famosos cuellos de botella, provocando un mal rendimiento global a pesar de contar con algunas tecnologías para evitar estas situaciones.

3.3.8 Información no realista de la estructura del Data Center: El inventario de los servidores se llevaba manualmente en una planilla de Excel. Muy difícil de seguir, muchos usuarios accedían a esa planilla, no solo para consultarla, sino también para actualizarla. Esa planilla no estaba del todo centralizada, se volvió inmanejable. Había varias versiones que no coincidían y casi nunca se tenía certeza total sobre la información real del Data Center. Sin información real de la estructura TI, es muy difícil que se tomen decisiones correctas que ayuden a mejorar la performance. Otra de las tareas que por el día a día, no se le daba la importancia necesaria

3.3.9 Limitada administración remota de los hosts físicos: Varios inconvenientes de los servers se debían solucionar in situ. La cantidad de servers era grande, con más de 15 racks. Muchos inconvenientes eran producto de los servidores que llevaban años de ser obsoletos y con sistemas que muy complicados de migrar. Esto aumentaba la probabilidad de errores que en la mayoría de los casos debían ser tratados de manera presencial en el Data center.

3.4 Inconvenientes en la gestión en un Centro de Dato descentralizado

En un Data Center no centralizado, con servidores y servicios independiente, la administración se vuelve muy compleja y costosa. Es difícil de escalar y mantener, presenta mayor riesgo operativo, más downtime y mayor costo operativo, lo que lo hace no muy adecuado para entornos modernos o críticos.

3.4.1 Gran complejidad en la administración de servidores independientes.

Cada servidor físico tenía su propio sistema operativo o Hypervisor. Aplicaciones aisladas, configuraciones manuales, monitoreo independiente. Genera un mantenimiento lento, no colabora con la estandarización y aumenta la probabilidad de errores humanos.

3.4.2 Aumento de downtime y discontinuidad del negocio

Los servidores físicos dedicados y servidores con hipervisores pero independientes, tienen el problema que si alguno falla, sus aplicaciones quedaban caídas hasta repararlo.

No había mecanismos automáticos para mover cargas a otros equipos. Había servidores con saturación de sus recursos y otros que estaban de manera holgada. Balancear la sobrecarga era imposible.

Otro inconveniente que provocaba esta situación es que un porcentaje importante de los servers ya cumplieron hace rato su tiempo de vida útil, con mucha degradación de funcionamiento.

Donde solo tenía soluciones muy precarias, porque se reemplazan sus piezas por otras de servers que ya estaban dado de baja.

3.4.3 Inconvenientes para implementar nuevos sistemas y agregar nuevos servidores.

Implementar nuevos sistemas muchas veces implicaba la compra de un servidor físico. O se destinaba a implementarlo en alguno de los servidores, pero que en su mayoría estaban con un funcionamiento muy comprometido. Esto influía directamente en el tiempo de entrega que era muy significativo, podía llevar semanas o meses. Esto es un claro ejemplo de una escalabilidad muy limitada

3.4.4 Problemas con el almacenamiento.

Con el pasar del tiempo el almacenamiento crece desproporcionadamente, es decir que muchos discos tienen almacenamiento saturado y otros con alto porcentaje de espacio libre. Una buena práctica en estas situaciones es distribuir las cargas, es decir mover sistemas de un server a otro para que la proporción de espacio libre en todos los dispositivos sea medianamente pareja. Estos tipos de data centers no cuentan con herramientas automáticas para migrar servidores, se debe hacer manual. Sumado a que los servers no estaban para nada integrados, por lo que se tornaban tareas muy costosas, y que no siempre se podían aplicar tan directamente. Solucionarlo implicaba downtime muy prolongados. Todo se realizaba manualmente y planificado con mucha antelación.

Otro problema de almacenamiento es contar con servidores muy viejos, la vida útil de sus discos ya habían pasados unos buenos años. Si se rompía un disco, generaba muchos inconvenientes en los sistemas alojados en ese servidor físico, y en el peor de los casos los servers no levantaban.

Si bien la mayoría de los hipervisores cuentan con la herramienta de snapshots, que facilita implementar modificaciones en los sistemas, por su facilidad de rollback en caso de no funcionar. El problema con los servers limitados de espacio, no era posible realizar snapshots.

Cada servidor con su almacenamiento local, provocaba una gran limitación: Una aplicación quedaba “atrapada” en su servidor físico. Otro factor que limitaba la escalabilidad.

3.4.5 Inconvenientes para una buena política de seguridad y control

Cualquier tipo de Data Center, ya sea centralizado o no, es vulnerable a ciberataques. Pero se amplifican los riesgos cuando el control no es centralizado, con mayor vulnerabilidad a accesos no autorizados, inconsistencia en protocolos de seguridad entre nodos, dificultad para monitorear amenazas en tiempo real, mayor exposición por estar cerca del usuario (ataques de proximidad) y problemas de gestión de credenciales, lo que aumenta la superficie de ataque y la complejidad de la defensa multicapa,

Si bien existía una política de permisos centralizada, convivía con la administración informal e individual de cada host. La mayoría de los hosts se administran con usuarios locales, con configuraciones manuales y muy diversas, por lo que dificulta mantener estándares de roles y permisos que replicaran en todos los servers.

Gestionar un control de acceso y vigilancia en data center no centralizados, es muy costoso y complejo, y sin buenos resultados. Con mucha vulnerabilidad, difícil de mantener con el tiempo y poca robustez.

3.4.6 Inconveniente para aplicar actualizaciones.

En un Data Center, se debe actualizar constantemente el Hardware (servidores, almacenamiento, redes) y el Software (sistemas operativos, aplicaciones, seguridad) para mejorar rendimiento, seguridad y eficiencia. Es un mantenimiento proactivo y estratégico.

Los mayores inconvenientes en este tipo de Data Centers para aplicar actualizaciones se dan por la complejidad logística, inconsistencia de versiones entre sitios, riesgos de seguridad por la dispersión y la dificultad para estandarizar políticas, lo que aumenta los tiempos de inactividad potenciales y la necesidad de coordinación, afectando la escalabilidad.

Un ejemplo claro es la aplicación de parches de un sistema operativo en una VM o en un host físico ya sea dedicado o con hipervisor. Como la descentralización provocaba muchos inconvenientes para un buen mantenimiento, era muy común que a Sistemas Operativos casi nunca se les aplicara parches de actualización del sistema. En casos como este, querer realizar el parchado para dejar el SO al día, con soluciones y mejora de performance e nivel de esa capa, generaba muchos inconvenientes, El principal es que era muchísima la cantidad de parches a aplicar, si se aplicaban todos juntos, no solo que el proceso en si demoraba mucho más de lo previsto, sino que en varios casos el sistema operativo tardaba mucho en levantarse después del reinicio o directamente no levantaban. A partir de esas malas experiencias se planificó para que la aplicación de parches sea más gradual, el problema es que también generaba demoras y reinicios haciendo que el sistema no esté disponible por un buen tiempo, y no siempre era posible determinar el tiempo que iba tomar esos parchados. Además, tampoco aseguraba que el server levantara sin inconveniente. Resumiendo, aplicar actualizaciones y parchado generaba mucho estrés, no se sabía si el server quedaría bien, provocaba alto downtime, no había una facilidad para generar una contingencia o respaldo, y esto colaboraba a que las planificaciones se dilataran mucho tiempo, generando mayores desactualizaciones y complicando más una solución adecuada. Prácticamente se trabajaba con intentar detener una bola de nieve.

Situación muy similar sucedía al pretender actualizar firmware y drivers de los servidores físicos, Generando los mismos problemas de riesgos, como procesos más prolongados de lo esperado o que el server no levantara.

Las actualizaciones que son muy importantes de aplicar para colaborar con el buen funcionamiento del Data Center, se transformaron en tareas evitables por la gran cantidad de inconvenientes que generaban. Esto dificultaba aún más, su administración.

3.4.7 Problema para implementar alertas y monitoreo y lograr una buena observabilidad.

En data centers descentralizados hay fragmentación de la visibilidad y sobrecarga de alertas. Con falta de estandarización y coordinación, genera una respuesta tardía de los incidentes y aumenta el riesgo de fallos.

Ante tanta diversidad de configuración causa que eventos críticos se procesen de forma desfasada, perdiendo el criterio de prioridad.

Cada host tiene su propio sistema de monitoreo, y muchos no tienen la opción de configurar alertas para enviarse por mail (mediante SMTP). Monitorear esos servers requiere en la mayoría de los casos, revisar la propia consola del host. Como consecuencia, no se tiene visibilidad de inconvenientes ni estado de funcionamiento, retrasando la detección y resolución de incidentes. Otro factor que colaboraba con el aumento de downtime.

Este tipo de administración complica detectar la raíz del inconveniente, lo que colaboraba con soluciones provisionales para salir del momento, pero que no duran mucho. Estos problemas reiterativos no es fácil darle una solución definitiva.

La diversidad de hardware insume mucho tiempo a los administradores para gestionar tal complejidad, agravada además por carecer de la formación específica para todos los entornos. Otro grave inconveniente es ante la alta vulnerabilidad a ataques externos, que se torna difícil de detectar y detener.

Estos hechos muestran que un Data Center sin una gestión centralizada, pierde mucho la visión global de la estructura de TI. Es muy difícil detectar las anomalías y propicia a que se ocupe directamente de las fallas, sabiendo la mala performance que esto provoca.

3.4.8 Poca probabilidad de automatización de operaciones y mantenimiento

Administrar esta gran variedad de host físicos es prácticamente todo manual. Gestionar el almacenamiento, balancear cargas y actualizar firmware y SO, no era posible automatizarlos.

Para automatizar, es necesario una estandarización de la estructura, algo imposible en este tipo de estructuras. Es más, varios hosts con el mismo modelo y marca, tenían diferencias en SO y firmware. Hasta era un gran inconveniente aplicar automatizaciones sectorizadas.

Estas tareas no se hacen de manera regular, implican un gran retrabajo de los administradores. Situación que colaboraba con aumentar la baja performance.

3.4.9 Problemas en las cargas de trabajo, saturación de algunos servidores.

Tanto en servidores físicos como virtuales, había un desbalanceo en la carga de trabajo. Generando mal rendimiento de los servidores más demandados.

Los servidores, sobre todos los virtuales se creaban a partir de nuevas implementaciones y de acuerdo a los requisitos exigidos en su momento. Con el pasar del tiempo, muchos de esos servers cambiaban mucho en el uso de sus recursos. Algunos tenían un crecimiento desmedido e incontrolable, generando muy baja performance en sus prestaciones. Otros se quedaban con una asignación muy sobredimensionada. Generando desperdicios de recursos y que era muy difícil de detectar.

Si bien estos inconvenientes, sobre los recursos de un Server, ya sea muy acotado o muy sobredimensionados es muy común. Sobre todos porque varias implementaciones venían de proveedores externos que en muchos casos, pedían de más por las dudas. El problema principal es que en una estructura descentralizada, ajustar los recursos para un mejor aprovechamiento del hardware, no era tarea sencilla. Esos ajustes implican no disponer del sistema por un tiempo significativo, lo que lo hacía muy difícil para planificar. Y había casos mucho más complicados, algunos sistemas crecían tanto, que ya no era posible asignarle más recursos, ya sea porque la versión de SO no lo soportaba o porque en la estructura subyacente, ya no contaban con más recursos.

Esta situación provocaba un aislamiento de cargas de trabajo. La incorporación de nuevos recursos de hardware era la solución, pero migrar sistemas de tamaño magnitud y con software muy obsoleto, necesitaba una gran reingeniería que llevaba mucho tiempo concretarlo.

Estructuras descentralizadas y con una gran variedad de tecnologías, es muy difícil abordar las sobrecargas de trabajo, y además las potenciaba. La falta de documentación de procesos y una escalabilidad muy manual, se hacía muy complejo administrarlo.

3.4.10 Dificultad para implementar aislamientos de funcionalidad de servidores.

Como en toda entidad con mucho uso de sistemas informáticos en sus operaciones, es necesario contar con un buen ambiente de prueba para evaluar las nuevas implementaciones y evitar errores en el pase a producción.

En un ambiente descentralizado con las características descritas en puntos anteriores, el ambiente de prueba es muy rústico. Se usaban equipos que dejaban de usarse en producción, es decir que hablamos de estructuras muy obsoletas y con bajo rendimiento. Además de ser limitado, muchos sistemas no siempre era factible replicar el escenario de producción. Por lo que las pruebas se hacían sobre sistemas que diferían bastante al productivo. Esto implicaba la aparición de errores cuando se pasaba a producción.

Otro gran inconveniente en el ambiente de prueba, es la seguridad. Al ser muy limitado, no había un dominio que permita replicar las políticas de seguridad en producción, esto también colaboraba que al momento de implementar, saltaban muchos errores por la seguridad.

Además, colabora mucho con la informalidad, no hay un aislamiento total. Es un ambiente altamente vulnerable a ataques informáticos o virus. Produciendo una fácil puerta de acceso, con ponía en riesgo al resto de la infraestructura.

El mantenimiento era prácticamente nulo. Una estructura de test con estas características, colaboraba más con situaciones de downtime. Las nuevas implementaciones, en su mayoría de carácter urgente, se aplicaban con pruebas que no eran lo suficiente para garantizar la buena funcionalidad. Aparecían muchos errores de acceso, de compatibilidad, inconsistencia o que directamente no funcionara sin posibilidad de detectar el motivo. Era muy común que las implementaciones en producción venía acompañadas de rollback. Lo que generaba una gran resistencia a los cambios. No había fluidez a las transformaciones constantes que tiene toda organización.

3.5 Visión global de un Data Center no centralizado

Todos estos inconvenientes que se describieron contribuye a una estructura con muy baja performance. La complejidad de aplicar políticas de seguridad, de aplicar nuevas implementaciones, de migrar más fluidamente, de automatizar cargas de trabajo, de tener un buen monitoreo global, con alto porcentaje de downtime, es un claro ejemplo de una escalabilidad casi nula y una alta interrupción en la disponibilidad de sus servicios. Colabora a no ocuparse de tomar medidas proactivas que eviten llegar a las fallas. Sino que siempre se va detrás de los problemas. Termina siendo una estructura gobernada por los incidentes, que se trabaje solamente solucionando inconvenientes y no ocuparse para implementar mejoras.

Una organización cuyo negocio depende de la disponibilidad de sus servicios, de la oferta constante a sus clientes, de innovar sus prestaciones y de adaptarse fácilmente a los cambios constantes del mercado, necesita de una infraestructura tecnológica que acompañe perfectamente ese comportamiento deseable. Que permita cambiar fácilmente, que este siempre funcionando, que el usuario perciba simpleza y agilidad en el uso de sus productos. Que haya practicidad para innovar. Una estructura que mitigue todas estas necesidades, difiere mucho de las prestaciones de Data Center descentralizado.

CAPÍTULO 4

Implementación de un Data Center Virtual Centralizado

4.1. Introducción

En este capítulo trataremos, sin entrar en tanto detalle, todo lo que se debe tener en cuenta para implementar un Data Center virtual, administrado por vSphere vCenter Server, con las herramientas mínimas como HA y DRS en el cluster. Que son las grandes ventajas básicas que ofrece este modelo de Data Center..

4.2 Infraestructura Física de un Data Center Virtual centralizado

El hardware para un entorno productivo basado en vSphere se deben tener en cuenta tras grandes bloques: Servidores físicos, Almacenamiento y Red.

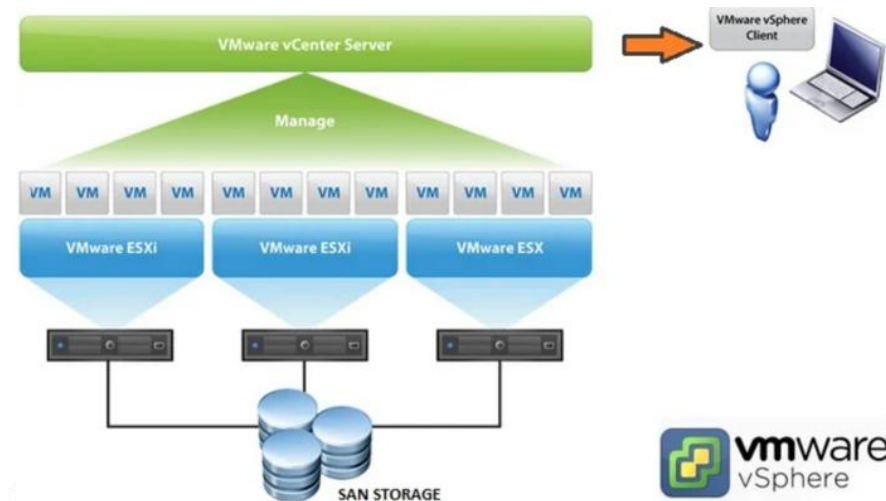


Figura 5. Estructura de VMware vCenter Server. Recuperada de (Manuel Serrano, 2021)

4.2.1 Servidores físicos (Hosts ESXi)

Los hosts deben ser compatible con VMware (HCL - Hardware Compatibility List). Entre los fabricantes habituales se encuentra Dell PowerEdge, HPE ProLiant, Lenovo ThinkSystem, Cisco UCS.

Requerimientos mínimos recomendados:

- CPU compatible con virtualización (Intel VT-x/EPT o AMD-V/RVI).
- 128 GB de RAM mínimo para producción (ideal 256–512 GB).
- Adaptadores de red de 10 GbE o superiores.
- Almacenamiento local NVMe/SSD para caché o vSAN.
- BMC para administración remota (iLO, iDRAC, IMM, CIMC).

Y si bien se puede comenzar con un mínimo de dos hosts, lo recomendable es comenzar con 3, para habilitar HA y DRS en cluster.

4.2.2 Almacenamiento / Datastores

Un Datastore es un repositorio de almacenamiento en el que se colocan las carpetas de nuestras máquinas virtuales. Estos datastores se utilizan para almacenar archivos VMDK (discos virtuales), configuraciones, ISOs y snapshots.

vSphere/vCenter gestiona almacenamiento a través de hosts ESXi utilizando principalmente datastores compartidos (SAN/NAS) o locales, soportando tecnologías VMFS (Virtual Machine File System), NFS (Network File System), vSAN (almacenamiento definido por software) y vVols (Virtual Volumes). Estas opciones permiten funciones avanzadas como vMotion, HA, DRS y Fault Tolerance.

Independientemente de llegar a través de un medio u otro, se puede trabajar a nivel de bloque y también trabajar con esos Datastores de tipo VMFS.

4.2.2.1 Los principales tipos de almacenamiento compatibles

- SAN (Storage Area Network) - A nivel de bloque
 - FC (Fibre Channel): Alta velocidad y rendimiento a través de red de fibra dedicada.
 - iSCSI: Utiliza Ethernet estándar para conectar almacenamiento a nivel de bloque.
 - FCoE (Fibre Channel over Ethernet): Encapsula tramas FC en redes Ethernet.
- NAS (Network Attached Storage) - A nivel de archivo
 - NFS (v3 y v4.1): Almacenamiento basado en archivos, fácil de configurar.
- Almacenamiento Local
 - Discos directos (SATA, SAS, NVMe) dentro de cada servidor ESXi, formateados con VMFS.
- Almacenamiento Definido por Software (SDS)
 - VMware vSAN: Agrupa discos locales de los hosts para crear un datastore compartido.
 - vVols (Virtual Volumes): Permite que la cabina de almacenamiento gestione máquinas virtuales nativamente a nivel de archivo/bloque [9].

4.2.3 Red (Switching y Routing)

La red física compuesta por switches, routers y firewalls que soportan la comunicación de los servidores y el centro de datos.

Redes físicas

- Cableado estructurado: Todo el cableado de cobre y fibra óptica que conecta servidores, switches, almacenamiento y otros dispositivos dentro del centro de datos. El diseño del cableado es crucial para el rendimiento y la escalabilidad, y el uso de pisos elevados facilita su organización y gestión.
- Switches: Dispositivos de red que conectan múltiples servidores y dispositivos dentro del mismo centro de datos. Para la gestión de vCenter, es fundamental tener switches de alta velocidad y capacidad de redundancia para garantizar la comunicación y el vMotion (migración de máquinas virtuales entre hosts).
- Routers: Conectan el centro de datos con redes externas, como la red de la empresa o Internet. Son esenciales para el acceso a los recursos y la comunicación entre el centro de datos y el mundo exterior.
- Firewalls: Dispositivos de seguridad que controlan el tráfico de red para proteger el centro de datos de amenazas externas. Se configuran para permitir o denegar el paso de datos en función de reglas de seguridad predefinidas.

- Infraestructura de administración: vCenter Server se implementa como un dispositivo virtual que debe tener su propia red de administración, a menudo con una dirección IP estática, para ser accesible y gestionar los hosts y las máquinas virtuales.

Switches 10GbE o superiores para tráfico: Management, vMotion. Almacenamiento (iSCSI/NFS/vSAN), Tráfico de Máquinas Virtuales

VLANs para segmentación:

- VLAN 10 – Management ESXi
- VLAN 20 – vMotion
- VLAN 30 – vSAN / Storage
- VLAN 40 – VMs producción
- VLAN 50 – vCenter Appliance [10]

Servicios de red: Una red virtual proporciona varios servicios al host y a las máquinas virtuales. Puede habilitar dos tipos de servicios de red en ESX:

- Conexión de las máquinas virtuales a la red física y entre ellas.
- Conexión de los servicios de VMkernel (como NFS, iSCSI, vSAN o vMotion) a la red física [11].

Configuración de VLAN: Las LAN virtuales (VLAN) permiten que se aisle aún más un único segmento LAN físico para que los grupos de puertos se aislen los unos de los otros como si estuvieran en segmentos físicamente diferentes.

VLAN en vSphere: La configuración de VLAN en un entorno de vSphere aporta ciertos beneficios.

- Integra los hosts ESX en una topología de VLAN previa.
- Aísla y protege el tráfico de red.
- Reduce la congestión del tráfico de red [12].

4.3 Sistema de instalación

Para comenzar con la implementación de un Data Center virtual administrador por vCenter, hay que comenzar a instalar el hipervisor ESXi en cada uno de los hosts. Es recomendable un mínimo de dos o tres host, para que las características de vMotion y HA, funcionen correctamente. Y para mayor performance, también es recomendable que todos los host sean mismo modelo y marca. Pero previamente a instalar el hipervisor, es recomendable configurar el Controlador de placas Bases

4.3.1 Controladoras de gestión de placas bases

Las controladoras de gestión de placas base, comúnmente llamadas BMC (Baseboard Management Controller), son microcontroladores especializados en servidores y sistemas de gama alta que permiten la monitorización y gestión remota del hardware fuera de banda (independientemente del SO y si el servidor está encendido), supervisa sensores, alerta errores del hardware, permite encendido, apagado y reinicio del server, actualiza firmware. Gestiona el sistema desde una red separada. Se puede acceder a la consola virtual del servidor Son esenciales para centros de datos, ya que un solo administrador puede gestionar muchos servidores de forma remota, reduciendo costos y mejorando la fiabilidad.

Algunos ejemplos:

- iDRAC (Integrated Dell Remote Access Controller) – Dell.
- iLO (Integrated Lights-Out) – HPE (Hewlett Packard Enterprise).
- XCC (XClarity Controller) / IMM (Integrated Management Module) – Lenovo
- Soluciones para Servidores Genéricos (OEM/ODM)

4.3.2 Instalación de ESXi en un servidor

En primer lugar, debe instalar hosts ESXi. Deben preparar los servidores físicos para la instalación. Se usará a modo de ejemplo un servidor Dell PowerEdge R740.

4.3.2.1 Configuración de BMC

Para configurar el iDRAC en un Dell PowerEdge R740, puedes usar el panel LCD del servidor o la utilidad del BIOS (F2), conectando un cable de red al puerto dedicado y eligiendo entre DHCP o IP estática, definiendo la IP, máscara y gateway, para luego acceder vía web con las credenciales root/calvin si no se han cambiado.

Hay dos métodos para definir el iDRAC: Usando el Panel LCD o desde el BIOS (F2)

Acceso Web (Después de la configuración)

Conecta un cable de red al puerto iDRAC dedicado. Abre un navegador y escribe la IP que configuraste (ej. <https://192.168.1.120>). Luego Inicia sesión con root (usuario) y calvin (contraseña, a menos que se haya cambiado).



Figura 6. Panel de iDRAC 9. Recuperada de (Dell, 2025)

4.3.2.2 Uso del visor de la consola virtual de iDRAC

El visor de la consola virtual proporciona varios controles. Estas incluyen la sincronización con el mouse, el escalamiento de la consola virtual, las opciones de chat, las macros del teclado, las acciones de alimentación, los dispositivos de próximo arranque y el acceso a la función de medios virtuales.

Los medios virtuales permiten que el servidor administrado tenga acceso a dispositivos de medios en la estación de administración o a imágenes de CD/DVD ISO en un recurso compartido de red como si fueran dispositivos en el servidor administrado. Utilizar la función de medios virtuales para acceder de manera remota a la instalación de las aplicaciones, actualización de controladores e instalación de un sistema operativo en el sistema administrado

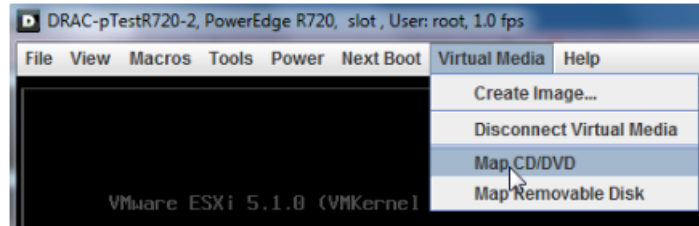


Figura 7. CD/DVD de Medios Virtuales y Mapas. Recuperada de (Dell, 2025)

4.3.3 Proceso de Instalación del ESXi

En cuanto a la versión del ESXi, siempre es recomendable que sea la última compatible con el modelo del host. Por ejemplo para un equipo Dell PowerEdge 740, la última compatible es la versión 8.0. Los instaladores se encuentran en la página oficial de VMware. Habilitado y configurado el iDRAC, se puede acceder remotamente al server antes de instalarle el hipervisor. Todos los hosts que se usarán en un cluster deben estar ubicados en el rack, con conexión de FC de HBA y conexión LAN para la administración y el iDRAC.

Por ejemplo, si se comienza a armar un cluster de producción con tres hosts. Se instalará ESXi en c/u. Además de instalar varias VM en cada uno de los servidores, en uno de ellos se debe desplegar vCenter Server Appliance. Después se pueden añadir más hosts ESXi para aumentar la capacidad de procesamiento con más VMs instaladas

Los principales componentes de instalación y configuración de vSphere son [13]:

ESXi 1: 192.168.11.30	vCenter: 192.168.11.31
ESXi 2: 192.168.11.27	Puerta de enlace/DNS: 192.168.11.2
ESXi 3: 192.168.11.32	Red: 192.168.11.0/255.255.255.0

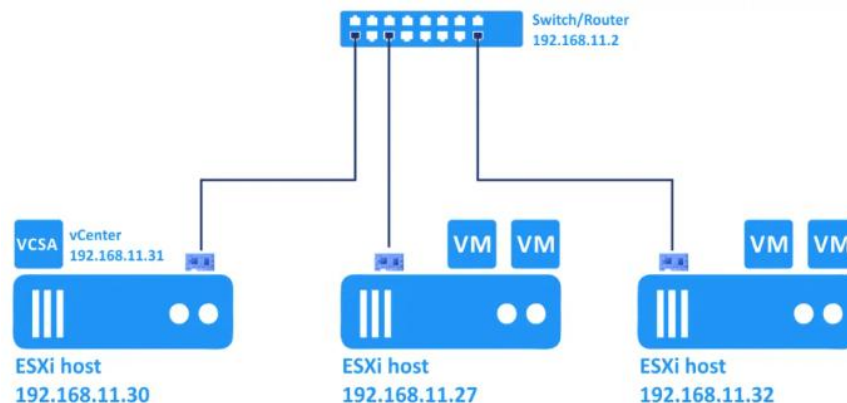


Figura 8. Estructura de un cluster. Recuperada de (Nakivo, 2024)

4.3.3.1 Instalación del primer host ESXi

Vamos a instalar el primer host ESXi (192.168.11.30) donde se desplegará la máquina virtual vCenter. La imagen ISO (VMware-VMvisor-Installer-7.0.0-15843807.x86_64.iso) se monta al DVD por consola a través de Virtual Media y arranque desde este medio preparado para ejecutar el instalador de ESXi 7 en su servidor.

Bienvenido a la instalación de VMware ESXi 7.0.0. Lea el mensaje de bienvenida y pulse Intro para continuar.

Seleccione un disco para instalar o actualizar. En este ejemplo tenemos un disco para instalar ESXi 7.0. Más tarde puedes conectar más discos, inicializarlos y utilizarlos como almacenes de datos para guardar los archivos de la máquina virtual. Seleccione un dispositivo de almacenamiento y pulse **Intro**.

Seleccione una distribución de teclado. En nuestro caso se utiliza *US Default*. Le recomendamos que utilice la misma opción.

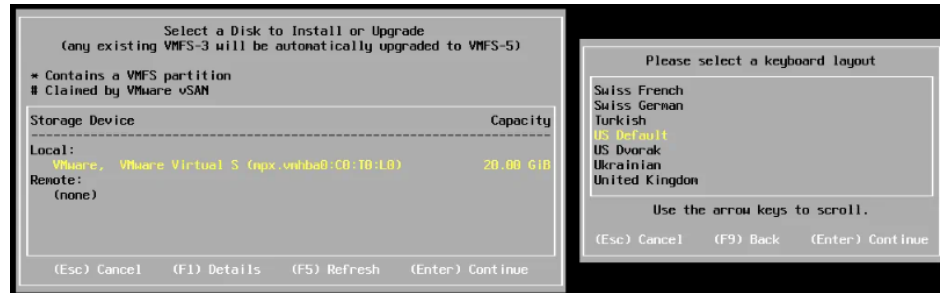


Figura 9. Contrato de Licencia. Recuperada de (Nakivo, 2024)

Introduzca una contraseña de root. La contraseña debe cumplir los requisitos de complejidad.

Confirme la instalación. Pulse F11 para iniciar el proceso de instalación de ESXi 7.0 en su servidor.



Figura 10. Contraseña de root. Confirmación de instalación. Recuperada de (Nakivo, 2024)

Instalación completada. Cuando vea esta pantalla, significa que ESXi 7.0 se ha instalado correctamente. Retire el medio de instalación y pulse **Intro** para reiniciar la máquina.

4.3.3.2 Configuración básica del host ESXi

Una vez que haya instalado ESXi 7.0 en su servidor verá una pantalla gris y amarilla que se llama *ESXi direct console* (DCUI). En esta pantalla puede ver la versión de ESXi, el número de compilación, la CPU, la configuración de la memoria, la dirección IP y un enlace que puede abrirse en un navegador web para gestionar el host ESXi.

Pulse **F2** para personalizar el sistema.

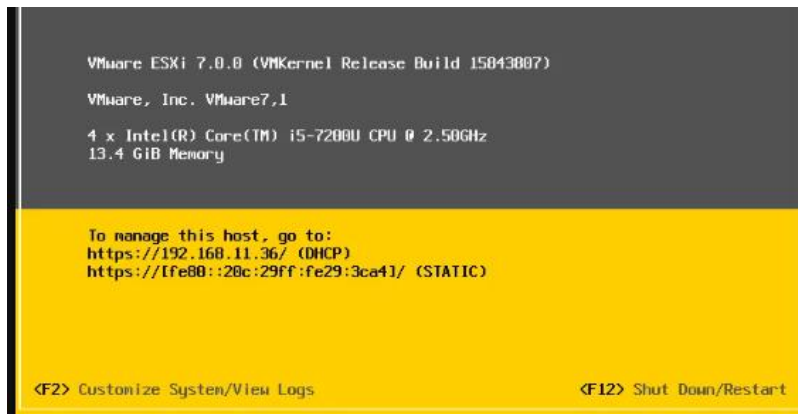


Figura 11. Consola directa del host ESXi –DCUI. Recuperada de (Nakivo, 2024)

Se requiere autenticación. Introduzca la contraseña de root que ha configurado durante la instalación de ESXi. Pula **Intro** para continuar.

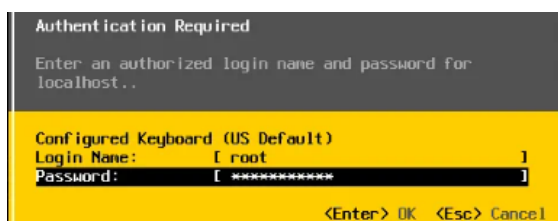


Figura 12. Pantalla de “Requiere Autenticación” en DCUI. Recuperada de (Nakivo, 2024)

Ahora se encuentra en el menú *Personalización del sistema*. En la parte derecha de la interfaz puede ver la dirección IP actual asignada mediante DHCP. Vamos a editar los ajustes de red y configurar una dirección IP estática en este host ESXi. Seleccione **Configurar red de gestión** y pulse **Intro**.

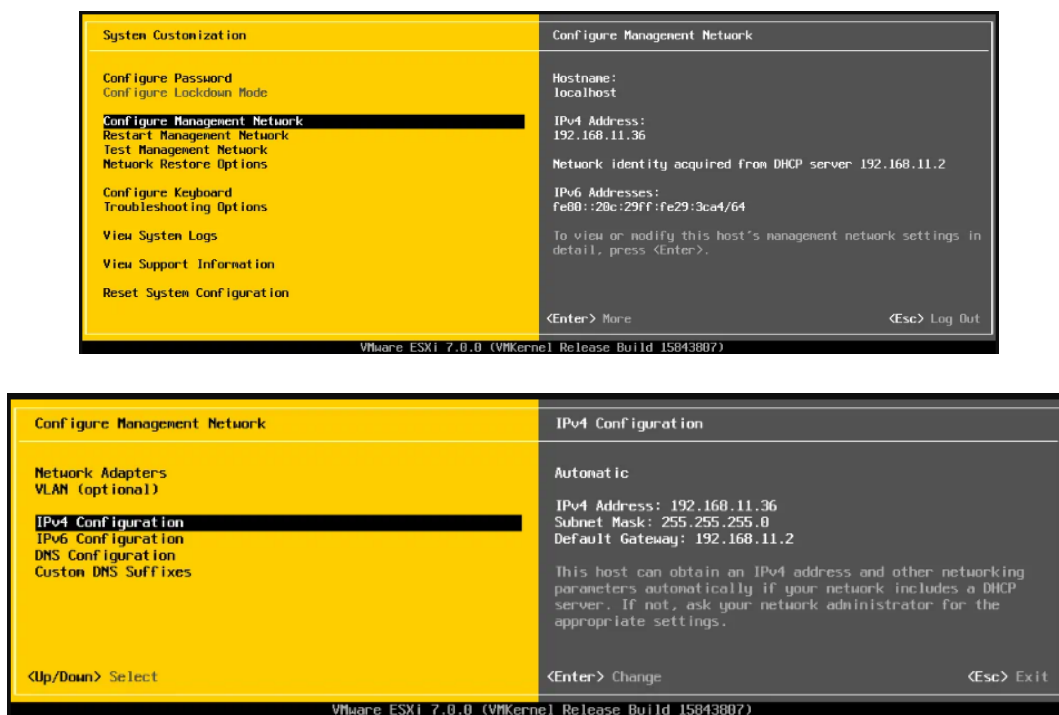


Figura 13. Configuración de red en DCUI. Recuperada de (Nakivo, 2024)

Introducimos los siguientes ajustes de IPv4:

Dirección IPv4: *192.168.11.30*

Máscara de subred: *255.255.255.0*

Puerta de enlace predeterminada: *192.168.11.2*

Pulsamos **Intro** para guardar los ajustes. Y se puede desactivar IPv6.

En la Configuración DNS, se configura como Servidor DNS primario: *192.168.11. 2*, DNS alternativo: *192.168.11.1* y nombre de host: *ESXi-30*

Es necesario reiniciar para aplicar los cambios.

Después de reiniciar el host ESXi, vaya a **Opciones de solución de problemas** en el *menú Personalización del sistema*.

Habilitar el acceso **ESXi Shell** y **SSH** para el host ESXi seleccionando la opción adecuada y pulsando **Intro** [13].



Figura 14. Habilitación de SSH por DCUI. Recuperada de (Nakivo, 2024)

4.3.4 Despliegue de VMware vCenter Server Appliance (VCSA)

Implementar VMWare vCenter Server, es mediante el vCenter Server Appliance, que es una máquina virtual preconfigurada y optimizada para ejecutar vCenter Server y los componentes de vCenter Server. Puede implementar la instancia de vCenter Server Appliance en hosts ESXi o instancias de vCenter Server [14].

El paquete de **vCenter Server Appliance** contiene el siguiente software:

- Photon OS® 3.0
- Los servicios de autenticación de vSphere
- PostgreSQL
- Extensión de VMware vSphere Lifecycle Manager
- VMware vCenter Lifecycle Manager
- Ver distintos appliance de vSphere que permiten administrar el cluster

Durante la implementación, puede seleccionar el tamaño de vCenter Server Appliance para el tamaño del entorno de vSphere y el tamaño de almacenamiento para los requisitos de base de datos [15].

El instalador de vCenter Server contiene archivos ejecutables para implementaciones de GUI (Interfaz gráfica) y CLI (Líneas de comandos).

- La **implementación de GUI** es un proceso de dos etapas. En la primera etapa, un asistente de implementación implementa el archivo OVA para el dispositivo en el host ESXi destino.

Una vez completada la implementación de OVA, el usuario es redirigido a la segunda etapa del proceso en la que se instalan y se inician los servicios del dispositivo recién implementado. Este método es el que más comúnmente se usa.

- El método de **implementación de CLI** implica ejecutar un comando de CLI en un archivo JSON preparado previamente. El instalador de CLI analiza los parámetros de configuración y los valores indicados en el archivo JSON, y genera un comando de OVF Tool para implementar y configurar automáticamente el dispositivo. La implementación de la CLI ejecuta automáticamente la etapa 1 y luego la etapa 2, sin necesidad de interacción del usuario.

vCenter Server Appliance tiene los siguientes nombres de usuario predeterminados:

root: Utilice este nombre de usuario para iniciar sesión en el sistema operativo del dispositivo y la interfaz de administración de vCenter Server.

La contraseña se establece durante la implementación del dispositivo virtual.

administrator@su_nombre_de_dominio Utilice este nombre de usuario para iniciar sesión en vCenter Single Sign-On.

La contraseña se establece durante la creación del dominio de vCenter Single Sign-On. El dominio de vCenter Single Sign-On se crea durante la implementación de una instancia de vCenter Server Appliance en un dominio de vCenter Single Sign-On nuevo.

Solo el usuario administrator@su_nombre_de_dominio contará con los privilegios necesarios para iniciar sesión en vCenter Single Sign-On y vCenter Server.

4.3.4.1 Requisitos de sistema para la nueva instancia de vCenter Server Appliance

Al usar nombres de dominios completos, asegúrese de que el equipo cliente que use para implementar el dispositivo y la red en la que se implementa utilicen el mismo dominio. Antes de implementar, sincronice los relojes del servidor de destino y todas las instancias de vCenter Server de la red de vSphere (servidor DNS) [16].

4.3.4.2 Requisitos de hardware para el dispositivo de vCenter Server

Los requisitos de hardware para vCenter Server Appliance dependen del tamaño del inventario de vSphere.

	Cantidad de vCPU	Memoria
Entorno muy pequeño (hasta 10 hosts o 100 máquinas virtuales)	2	12 GB
Entorno pequeño (hasta 100 hosts o 1.000 máquinas virtuales)	4	19 GB
Entorno mediano (hasta 400 hosts o 4.000 máquinas virtuales)	8	28 GB
Entorno grande (hasta 1.000 hosts o 10.000 máquinas virtuales)	16	37 GB
Entorno extragrande (hasta 2.000 hosts o 35.000 máquinas virtuales)	24	56 GB

Figura 15. Requisitos de hardware para una instancia de vCenter Server Appliance. Recuperada de (Broadcom, 2025)

4.3.4.3 Requisitos de almacenamiento para el dispositivo de vCenter Server

Los requisitos de almacenamiento son diferentes para cada tamaño de entorno de vSphere y dependen de los requisitos de tamaño de la base de datos.

	Tamaño de almacenamiento predeterminado	Tamaño de almacenamiento grande	Tamaño de almacenamiento extragrande
Entorno muy pequeño (hasta 10 hosts o 100 máquinas virtuales)	579 GB	1992 GB	4279 GB
Entorno pequeño (hasta 100 hosts o 1.000 máquinas virtuales)	694 GB	2046 GB	4304 GB
Entorno mediano (hasta 400 hosts o 4.000 máquinas virtuales)	908 GB	2140 GB	4468 GB
Entorno grande (hasta 1.000 hosts o 10.000 máquinas virtuales)	1358 GB	1958 GB	4518 GB
Entorno extragrande (hasta 2.000 hosts o 35.000 máquinas virtuales)	2283 GB	2383 GB	4620 GB

Figura 16. Requisitos de almacenamiento para una instancia de vCenter Server Appliance. Recuperada de (Broadcom, 2025)

4.3.4.4 Puertos necesarios en vCenter Server

El sistema vCenter Server debe poder enviar datos a cada host administrado y recibir datos de vSphere Client. Para permitir las actividades de migración y aprovisionamiento entre los hosts administrados, los hosts de origen y destino deben poder recibir datos entre sí a través de los puertos TCP y UDP predeterminados.

Se puede acceder a vCenter Server a través de los puertos TCP y UDP predeterminados. Para obtener la lista de todos los puertos y protocolos compatibles en vSphere, consulte la herramienta VMware Ports and Protocols™ en <https://ports.broadcom.com>. Algunos claves son:

- 443 (TCP): Interfaz web (vSphere Client) y comunicación HTTPS. Redirige desde el puerto 80.
- 902 (TCP/UDP): Puerto principal utilizado por vCenter para enviar datos a los hosts gestionados (ESXi) y para la consola de máquinas virtuales.
- 389 (TCP/UDP): Servicios de directorio (LDAP) para grupos de vCenter y comunicación con Active Directory.
- 636 (TCP): LDAP seguro (SSL) para el modo vinculado (Linked Mode).
- 22 (TCP): SSH para acceso de administración, principalmente en vCenter Server Appliance (VCSA).
- 514 (TCP/UDP): vSphere Syslog Collector.
- 5671 (TCP): Comunicaciones de la infraestructura de mensajes.

4.3.4.5 Guía de instalación de VMware vCenter y prácticas recomendadas

La forma más habitual de instalar vCenter es desplegar vCenter Server Appliance (VCSA) como máquina virtual en un host ESXi.

Aunque se pueden crear máquinas virtuales con una instalación gratuita de ESXi, se necesita vCenter Server para acceder a las funciones empresariales necesarias, sobre todo en entornos de misión crítica. La mayoría, si no todos, de los demás productos complementarios de VMware requieren vCenter. Por lo tanto, vamos ahora a la guía de instalación del servidor VMware vCenter.

4.3.4.5.1 Instalación y opciones de VMware vCenter

Tradicionalmente, existían dos opciones para la instalación de vCenter Server:

- en un servidor Windows, ya sea físico o virtual
- utilizando un appliance Linux OVA dentro del propio entorno virtual. El appliance se conoce como vCenter Server Virtual Appliance o VCSA.

En los primeros días de vCenter, se prefería una instalación de servidor Windows, ya que era, en ese momento, la plataforma con mejor rendimiento para vCenter. Sin embargo, con el desarrollo del appliance virtual despegando, VMware anunció que el VCSA es tan robusto como el appliance Windows. De hecho, se ha observado que VMware utiliza exclusivamente el VCSA internamente para gestionar sus propios recursos de máquinas virtuales.

La compatibilidad con la instalación de vCenter en Windows se interrumpió con vCenter 6.7. VMware vCenter 7.0 no admite la instalación en Windows y sólo puede instalarse como appliance virtual basado en Linux (Photon OS), también denominado VCSA. Por este motivo, en esta guía de instalación del servidor VMware vCenter, desplegamos vCenter como appliance virtual en un host ESXi. Este tutorial de instalación de vCenter es aplicable a vCenter 7 y 8.

Para instalar vCenter 7.0 o superior en un entorno vSphere, primero debe preparar un host ESXi.

4.3.4.5.2 Instalación de VMware vCenter Appliance

Echemos un vistazo a la instalación de un vCenter Server Virtual Appliance (VCSA) típico en nuestro entorno virtual:

1. Descargue el paquete de instalación de vCenter del sitio web de VMware. Tenga en cuenta que el enlace de descarga está disponible para los usuarios registrados de VMware. El VCSA descargado está en formato ISO y no en un archivo OVA.
2. Monte esta imagen ISO en un equipo Windows y ejecute el instalador de vCenter en la interfaz gráfica de usuario (GUI).

Como puede ver en la siguiente captura de pantalla, hemos montado la imagen ISO y ahora podemos ver su contenido. Tenemos que ejecutar el archivo **installer.exe** desde el Explorador de Windows. Este archivo lanzador para Windows se almacena en el directorio D:\vcsa-ui-installer\win32, donde D: es la unidad de DVD virtual en la que hemos montado la imagen de instalación ISO de vCenter. Para iniciar el instalador, haga doble clic en el archivo.

Del mismo modo, puede encontrar el instalador para ejecutarlo desde los sistemas operativos Linux y macOS en los subdirectorios lin64 y mac, respectivamente.

Tenga en cuenta que puede encontrar el archivo de plantilla OVA que se puede utilizar alternativamente para desplegar vCenter en una VM:

D:\vcsa\VMware-vCenter-Server-Appliance-7.0.0.10300-16189094_OVF10.ova

Este archivo OVA puede ser útil si despliega vCenter en un laboratorio doméstico de VMware. También es posible instalar VCSA en la interfaz de línea de comandos (CLI).

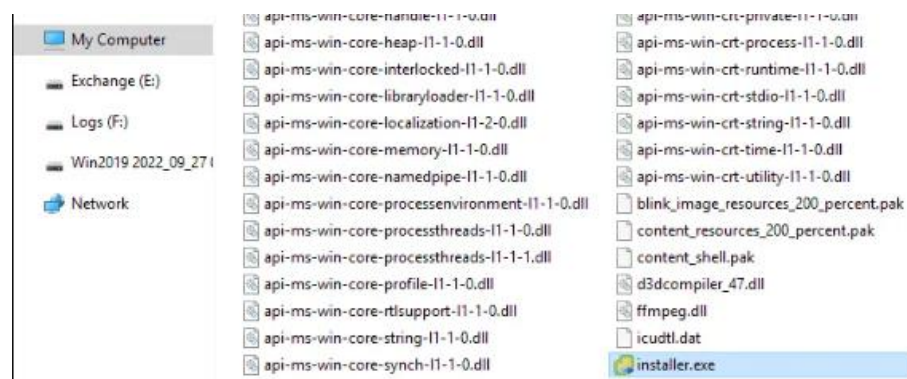


Figura 17. Archivo de instalación de VCSA. Recuperada de (Nakivo, 2024)

- 3- Una vez que se abra la ventana del instalador de vCenter, verá una página en la que podrá elegir entre Instalar, Actualizar, Migrar o Restaurar el appliance vCenter Server.

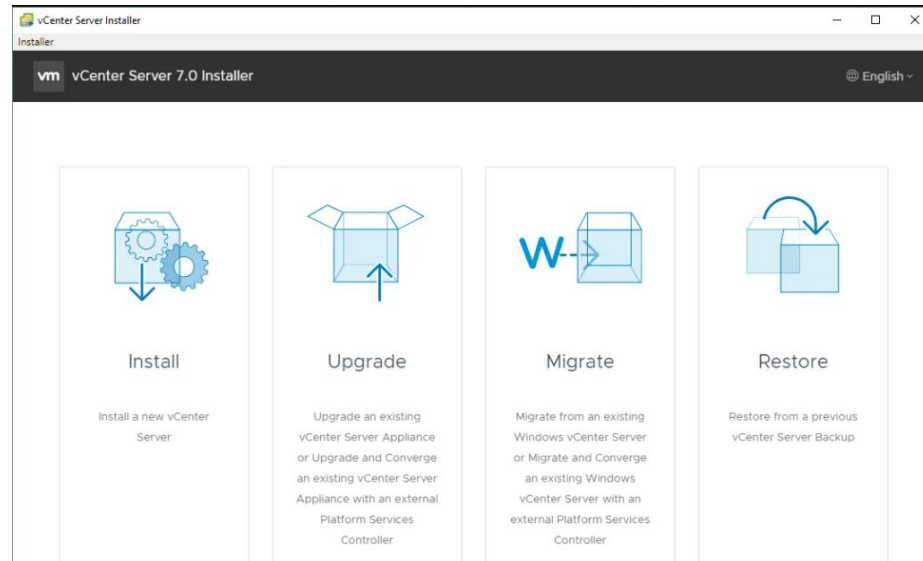


Figura 18. Asistente de instalación de VCSA. Recuperada de (Nakivo, 2024)

Haga clic en Instalar para instalar un nuevo appliance. El asistente de instalación de vCenter Server se abre en la ventana del instalador y comienza con la Etapa 1: Instalación de vCenter Server. Hay dos etapas en la instalación del servidor VMware vCenter.

4.3.4.5.2.1 Fase 1: Instalación de vCenter Server

1- Introducción. Lea la información que aparece en esta pantalla, incluida la notificación sobre el controlador de servicios de plataforma. Haga clic en Siguiente en cada paso del asistente para continuar.

El Controlador de Servicios de Plataforma contiene servicios compartidos como Single Sign-On, Licencias y gestión de certificados. Puede optar por alojar todo esto en el mismo appliance (servidor vCenter y controlador de servicios de plataforma).

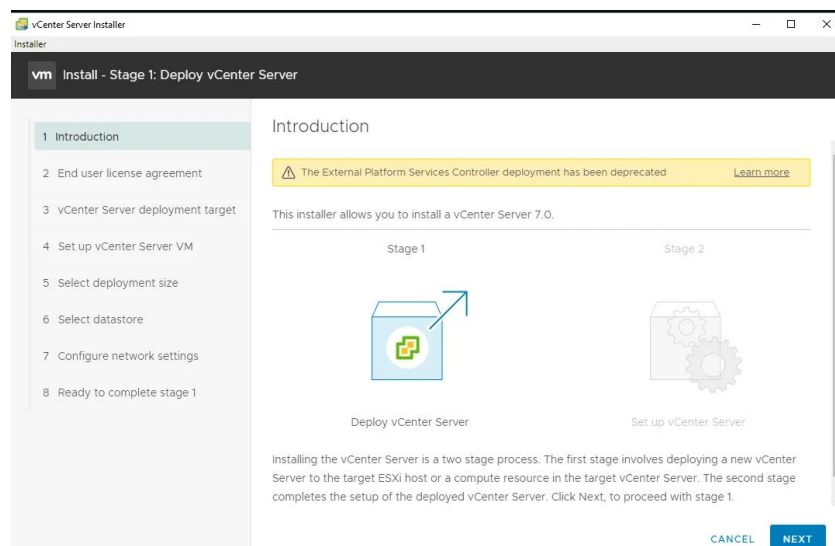


Figura 19. Asistente de instalación (Fase 1) de VCSA. Recuperada de (Nakivo, 2024)

2- Acuerdo de licencia de usuario final. La segunda pestaña que se encuentra es el CLUF (acuerdo de licencia de usuario final). Seleccione la casilla situada junto al mensaje Acepto los términos del acuerdo de licencia y haga clic en Siguiente.

3- Objetivo (destino) de instalación de vCenter Server. La siguiente pantalla de configuración es la pantalla de configuración del objetivo de instalación de vCenter Server. Esto le pedirá que rellene la información de conexión para conectarse al servidor ESXi host, que será el host en el que se aprovisione realmente la VM del appliance. Puede introducir una dirección IP o un FQDN (Fully Qualified Domain Name) y, a continuación, añadir las credenciales de usuario necesarias para conectarse al host.

Figura 20. Formulario donde se indica los datos del host donde se aprovisionará la VM de VCSA. Recuperada de (Nakivo, 2024)

Puede recibir una advertencia sobre el certificado del host si se utiliza un certificado autofirmado. Puedes simplemente aceptarlo y seguir adelante.

4- Configure vCenter Server VM. Ahora puede entrar más en los detalles de la configuración de la máquina virtual con el propio vCenter. Aquí se configura el nombre del appliance (nombre de la VM) y la contraseña del SO para el usuario root (un usuario root en un SO Photon basado en Linux utilizado para VCSA).

Figura 21. Especificar el nombre de la VM y la password root del VCSA. Recuperada de (Nakivo, 2024)

5- Seleccione el tamaño de la instalación. Este paso es una parte crucial del proceso de configuración. A continuación, el cuadro combinado se despliega para que pueda ver las opciones disponibles. Al seleccionar las distintas opciones, se asignan cantidades variables de recursos a la máquina virtual que se aprovisiona para vCenter.

Seleccionamos la opción Tiny en esta guía de instalación de VMware vCenter Server.

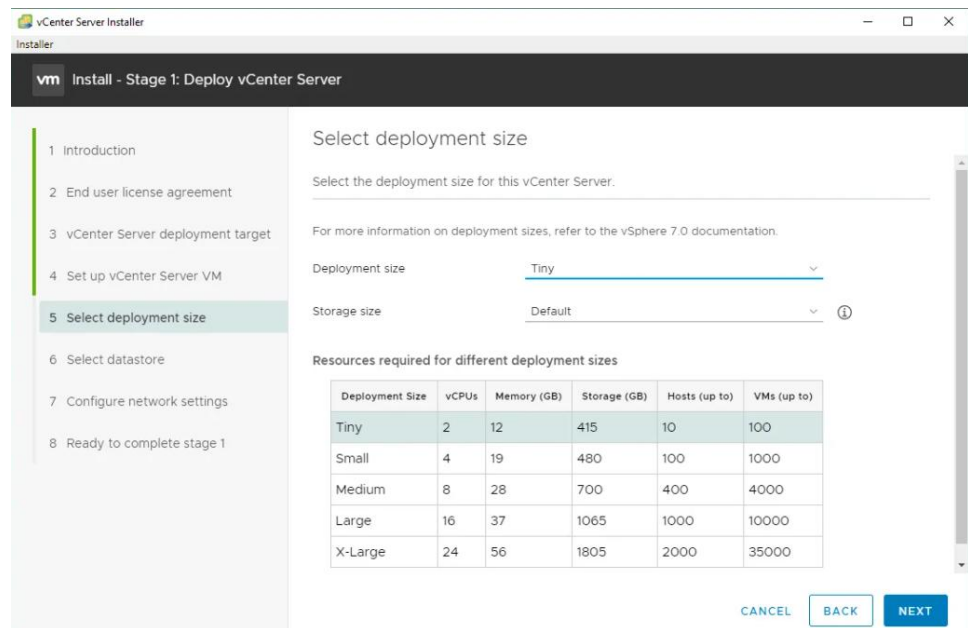


Figura 22. Seleccionar el tamaño de la instalación. Recuperada de (Nakivo, 2024)

6- Seleccione el almacén de datos. Estas son las opciones que debe configurar para que el host ESXi aprovisione la máquina virtual. Aquí se configura el almacén de datos de destino donde se desplegará el appliance vCenter.

Seleccione el almacén de datos necesario que contenga suficiente espacio de almacenamiento libre. Puede habilitar el modo de disco delgado para utilizar discos virtuales de aprovisionamiento delgado para la VM VCSA para ahorrar espacio de almacenamiento.

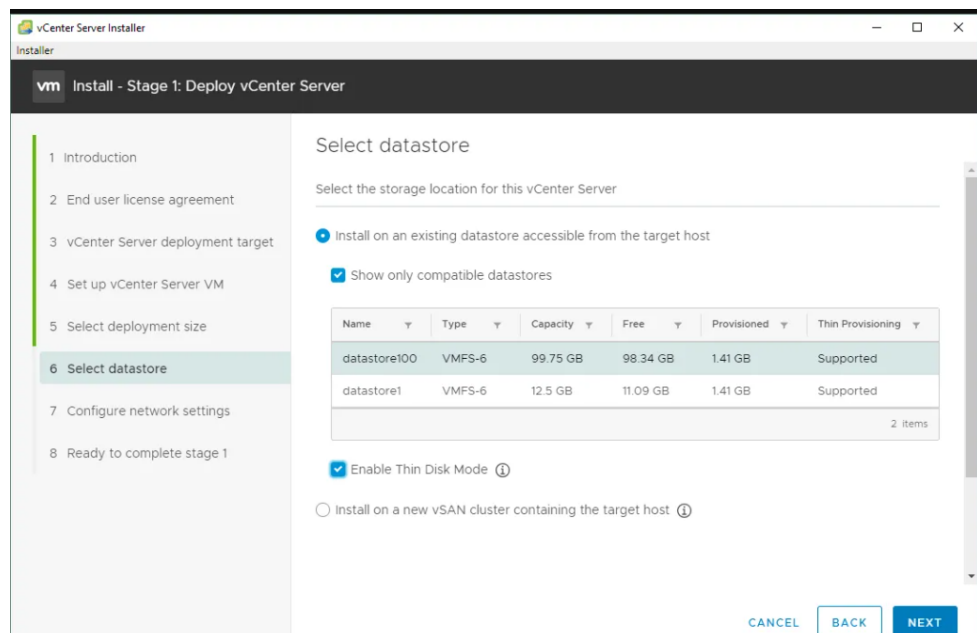


Figura 23. Seleccionar el repositorio donde se guardará la VM de VCSA. Recuperada de (Nakivo, 2024)

7- Configura los ajustes de red. Utilice la configuración IP estática. Es crucial que tenga un registro DNS que funcione para el nombre FQDN de su sistema, ya que la instalación fallará siempre si el FQDN no se puede resolver. Asegúrese de comprobarlo antes de seguir adelante.

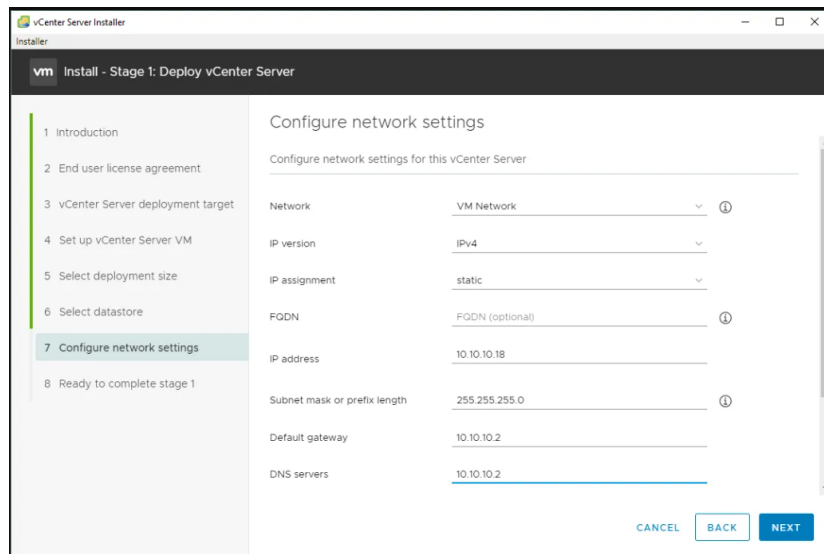


Figura 24. Especificar los datos de la red del VCSA. Recuperada de (Nakivo, 2024)

8- Listo para completar la fase 1. Este es el resumen de la configuración de la instalación de vCenter y las operaciones que deben realizarse para aprovisionar la máquina virtual del appliance. Compruebe los parámetros y haga clic en Finalizar para completar la etapa 1.

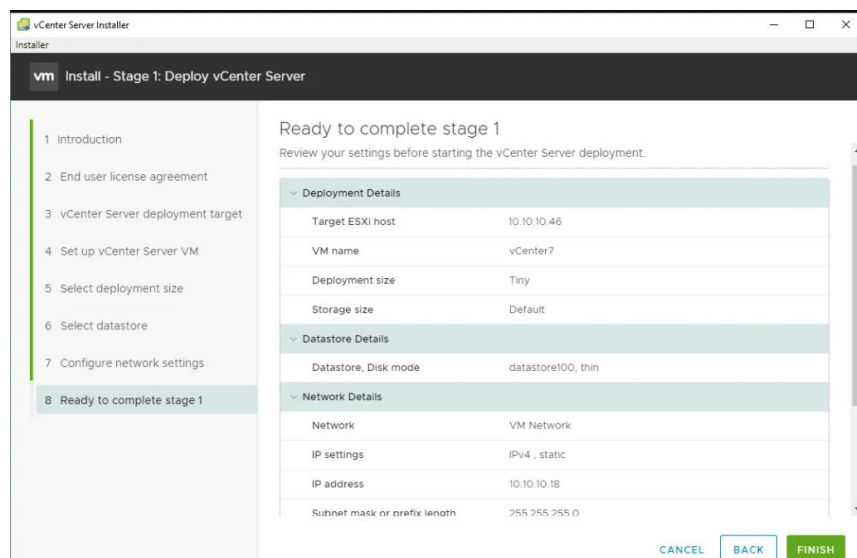


Figura 25. Muestra todos los parámetros configurados antes proceder con la instalación del VCSA. Recuperada de (Nakivo, 2024)

Una vez que haga clic en Finalizar, comenzará la operación de instalación para desplegar el OVA en su host ESXi y empezará a ver moverse el indicador de progreso.

Si no hay problemas en el proceso de instalación de vCenter, especialmente con DNS, debería recibir un mensaje sobre la correcta instalación del appliance.

Haga clic en Continuar para pasar a la **etapa 2**.

Etapa 1 se ha completado, y ahora tiene que completar la **Etapa 2** con la configuración del appliance vCenter Server. Preste atención al enlace a la interfaz de gestión de vCenter Server, como <https://vcenter7.localdomain:5480/> en nuestro caso. También puede utilizar este enlace para continuar con la fase 2 de la instalación de vCenter si cierra el asistente por cualquier motivo. [17]

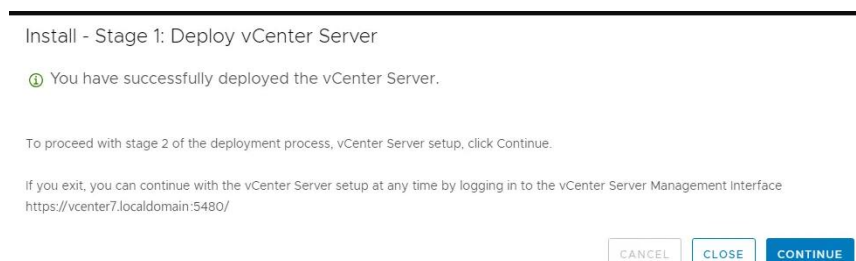


Figura 26. Pantalla de indicación de instalación exitosa de la Etapa1. Recuperada de (Nakivo, 2024)

4.3.4.5.2.2 Etapa 2: Configuración de vCenter Server

1- Introducción. Se le notifica que ha comenzado la fase 2 de la instalación de VMware vCenter Server. Haga clic en **Siguiente** para continuar.

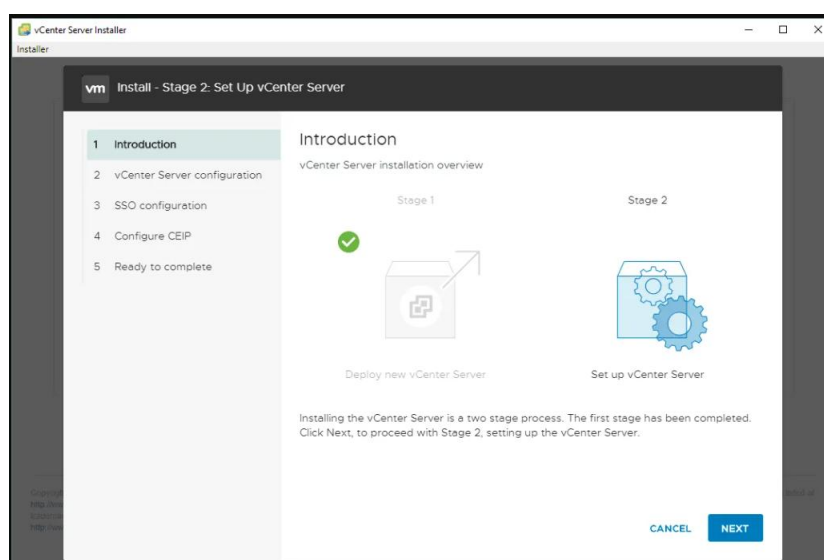


Figura 27. Inicio de instalación de la Etapa2. Recuperada de (Nakivo, 2024)

2- Configuración de vCenter Server. Seleccione el modo de sincronización horaria y habilite el acceso SSH a vCenter Server Appliance.

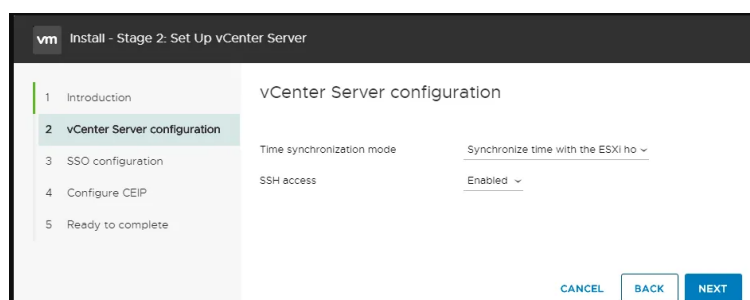


Figura 28. Sincronización horaria y acceso a SSH de VCSA. Recuperada de (Nakivo, 2024)

3- Configuración SSO. La configuración de SSO permite a vSphere autenticar sesiones de usuario en distintos servicios de autenticación de seguridad, como Active Directory, seguridad local u otro servicio de autenticación de seguridad SAML. Aunque no tenga previsto utilizar ninguna de estas otras fuentes, debe configurar SSO para instalar vCenter. Además, asegúrese de que su dominio SSO es diferente de su nombre de dominio de AD. El nombre de dominio SSO predeterminado **vsphere.local**.

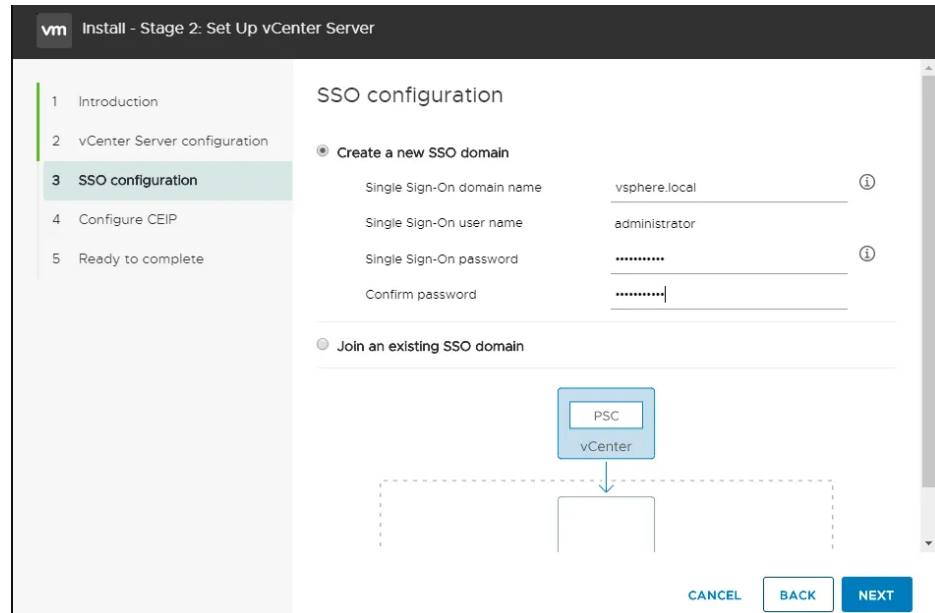


Figura 29. Configuración de SSO de VCSA. Recuperada de (Nakivo, 2024)

4- Configurar el CEIP. A continuación, puede optar por participar en el Programa de mejora de la experiencia del cliente de VMware. En este ejemplo, desmarcamos la casilla de verificación en este paso de la guía de instalación del servidor VMware vCenter.

5- Listo para completar. Compruebe su configuración y haga clic en Finalizar si todo es correcto para completar la etapa 2.

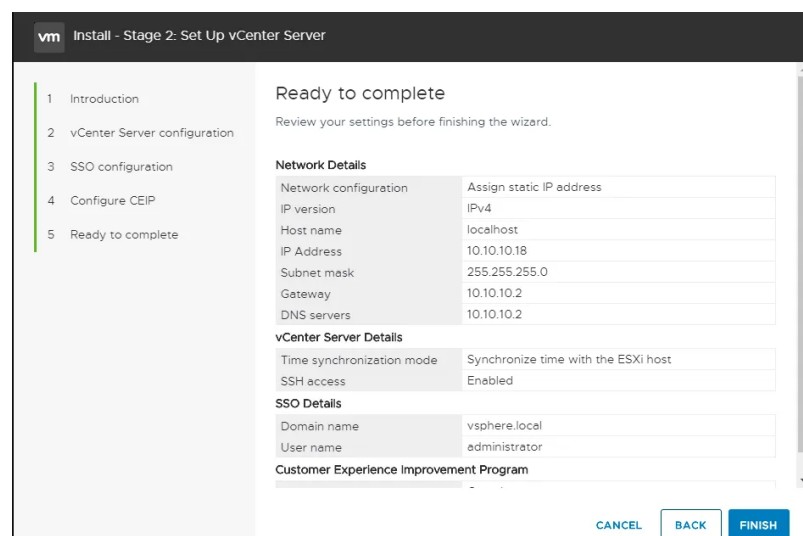


Figura 30. Lista de los parámetros configurados antes de aceptar el proceso de VCSA. Recuperada de (Nakivo, 2024)

6- Lea el mensaje de advertencia y tenga en cuenta que no puede detener ni pausar el proceso de instalación del servidor VMware vCenter. Pulse OK para continuar.

7- Espere a que finalice el proceso de instalación del servidor VMware vCenter.

8- Una vez finalizada la instalación de vCenter, puede abrir un navegador web e iniciar sesión en VMware vSphere Client introduciendo la dirección IP del VMware VCSA que ha configurado durante el proceso de instalación de vCenter. Nos dirigimos a <https://10.10.10.18> en un navegador web y utilizamos `administrator@vsphere.local` como nombre de usuario. Tenga en cuenta que ahora sólo está disponible el Cliente vSphere HTML5.



Figura 31. Pantalla inicial de la consola web de inicio del VCSA. Recuperada de (Nakivo, 2024)

9- Si ya ha adquirido la licencia de vCenter, puede introducir la clave de licencia de vCenter, añadir hosts ESXi al inventario de vCenter, crear máquinas virtuales, configurar clústeres y realizar otras acciones. Dispone de 60 días con la versión de prueba con todas las funciones para aplicar la licencia.

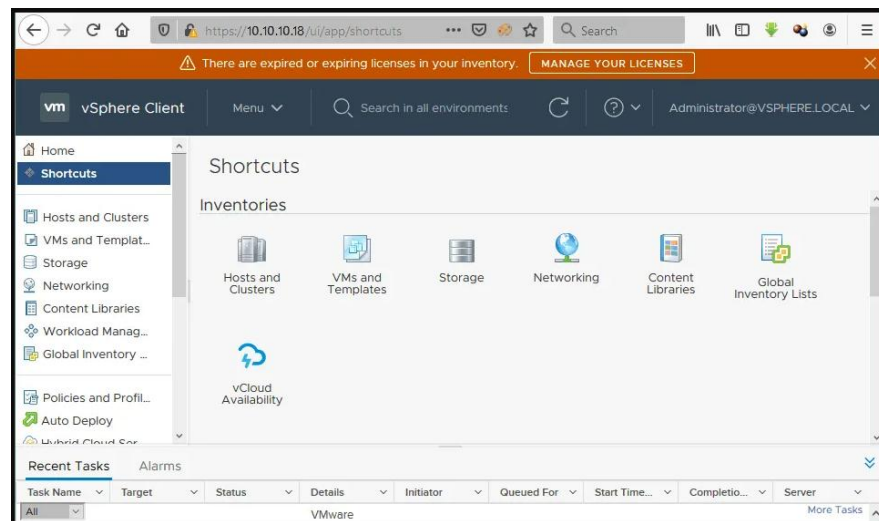


Figura 32. Vista de la consola web de vCenter Server. Recuperada de (Nakivo, 2024)

10- Vaya a https://<vCenterFQDN_or_IP>:5480 en su navegador web y establezca la fecha de caducidad de la contraseña raíz en los ajustes de administración (<https://10.10.10.18> en nuestro caso). Si su contraseña caduca, no podrá iniciar sesión en https://<vCenterFQDN_or_IP>:5480 que contiene algunos ajustes importantes de VCSA [17].

4.4 Crear Clusters de vSphere HA

Los clústeres de vSphere HA permiten que una colección de hosts ESXi funcionen en conjunto, de manera que, como grupo, proporcionen mayores niveles de disponibilidad para máquinas virtuales de lo que puede proporcionar de forma individual cada host ESXi. Cuando planifique la creación y el uso de un nuevo clúster de vSphere HA, las opciones que seleccione afectarán la manera en que el clúster responde a los errores de los hosts o las máquinas virtuales.

4.4.1 Funcionamiento de vSphere HA

vSphere HA ofrece alta disponibilidad para máquinas virtuales agrupando en un clúster las máquinas virtuales y los hosts en los que residen. Se supervisan los hosts en el clúster y, en caso de un error, las máquinas virtuales en un host con errores se reinician en hosts alternativos.

Cuando se crea un clúster de vSphere HA, automáticamente se elige un único host como el host principal. El host principal se comunica con vCenter Server y supervisa el estado de todas las máquinas virtuales protegidas y de los hosts secundarios. Es posible que haya diferentes tipos de errores del host, y el host principal debe detectar y corregir apropiadamente el error. El host principal debe distinguir entre un host con errores y uno que está en una partición de red o que ha quedado aislado de la red. Para determinar el tipo de error, el host principal utiliza la verificación de latidos de la red y del almacén de datos.

4.4.2 Hosts principales y secundarios en un cluster

Cuando agrega un host a un clúster de vSphere HA, se carga un agente al host que se configura para que se comunique con otros agentes del clúster. Cada host del clúster funciona como host principal o host secundario.

Cuando vSphere HA está habilitado para un clúster, todos los hosts activos (aquellos que no están en modo de espera o mantenimiento ni están desconectados) participan en una elección para seleccionar el host principal del clúster. El host que monta la mayor cantidad de almacenes de datos tiene una ventaja en la elección. Normalmente, solo existe un host principal por clúster y todos los otros hosts son secundarios. Si el host principal genera errores, se apaga o se coloca en modo de espera o se quita del clúster, se realiza una nueva elección.

El host principal de un clúster tiene varias responsabilidades:

- Supervisar el estado de los hosts secundarios. Si un host secundario genera errores o no se puede acceder a él, el host principal identifica qué máquinas virtuales deben reiniciarse.
- Supervisar el estado de energía de todas las máquinas virtuales protegidas. Si una máquina virtual genera errores, el host principal se asegura de que se reinicie. Mediante el uso de un motor de selección de ubicación local, el host principal también determina dónde debe realizarse el reinicio.
- Administrar las listas de hosts del clúster y máquinas virtuales protegidas.
- Actuar como la interfaz de administración de vCenter Server con el clúster e informar el estado del clúster.

Los hosts secundarios contribuyen principalmente con el clúster ejecutando máquinas virtuales a nivel local, supervisando sus estados de tiempo de ejecución y notificando actualizaciones de estado al host principal. Un host principal también puede ejecutar y supervisar máquinas virtuales. Tanto los hosts secundarios como los principales implementan las funciones de supervisión de máquinas virtuales y de aplicaciones.

Una de las funciones que realiza el host principal es orquestar reinicios de máquinas virtuales protegidas. Una máquina virtual se protege mediante un host principal después de que vCenter Server observe que el estado de energía de la máquina virtual ha cambiado de apagado a encendido en respuesta a una acción del usuario. El host principal mantiene activa la lista de máquinas virtuales protegidas en los almacenes de datos del clúster. Un host principal elegido recientemente utiliza esta información para determinar qué máquinas virtuales hay que proteger.

4.4.3 vSphere Cluster Services

vSphere Cluster Services (vCLS) es una funcionalidad introducida en VMware vSphere 7.0 Update 1. Esta característica garantiza que los servicios de clúster, como vSphere DRS y vSphere HA, estén todos disponibles para mantener los recursos y el estado de las cargas de trabajo que se ejecutan en los clústeres independientemente de la disponibilidad de la instancia de vCenter Server.

vSphere Cluster Services implementa máquinas virtuales de vSphere Cluster Services en cada clúster de vSphere. Las máquinas virtuales de vSphere Cluster Services se implementan en un clúster durante su creación y los hosts se agregan al clúster después.

VMware vSphere® Distributed Resource Scheduler® (vSphere DRS) no puede funcionar si las máquinas virtuales de vSphere Cluster Services no están presentes en el clúster de vSphere.

Los Servicios de Clúster de vSphere se habilitan para todos los clientes de 7U1 (vSphere 7.0 Update 1). Esta función se habilitará de forma predeterminada para todos los clientes de vSphere al actualizar a 7U1 o al realizar nuevas implementaciones.

La arquitectura de vSphere Cluster Services consta de un máximo de tres máquinas virtuales de agente que se implementan automáticamente. Estas máquinas virtuales ligeras forman un quórum de agentes de clúster. Para clústeres con menos de tres hosts, la cantidad de máquinas virtuales del agente es igual a la cantidad de hosts ESXi.

Las tres máquinas virtuales del agente se autocorrijen. Esto significa que, cuando no estén disponibles, vSphere Cluster Services intentará encenderlas automáticamente.

4.4.3.1 Máquinas virtuales del agente

Las máquinas virtuales de vSphere Cluster Services (vCLS) están presentes en cada clúster de vSphere y tienen las siguientes características:

- Administrado por vCenter Server
- Ejecute una instalación mínima de Photon OS.
- Configurado con 1 CPU virtual, 128 MB de memoria y 2 GB de disco con aprovisionamiento fino.
- No tiene una tarjeta de interfaz de red (NIC) o dirección IP asignada, utiliza la interfaz VMCI (Virtual Machine Communication Interface) para comunicarse con el hipervisor.
- Se implementan en un almacén de datos compartido. Cuando no hay un almacén de datos compartido disponible, las máquinas virtuales de vSphere Cluster Services se implementan en almacenes de datos locales.
- Implementado desde un OVA con un perfil mínimo instalado de Photon OS, vSphere Cluster Services administra los recursos, el estado de energía y la disponibilidad de estas máquinas virtuales.
- No se admite la modificación de las máquinas virtuales de vSphere Cluster Services

Para los clientes de vSphere, las máquinas virtuales de vSphere Cluster Services no son visibles en el árbol de inventario de la vista Hosts y clústeres. En su lugar, las verá en la vista Máquinas virtuales y plantillas, como se muestra a continuación [18].

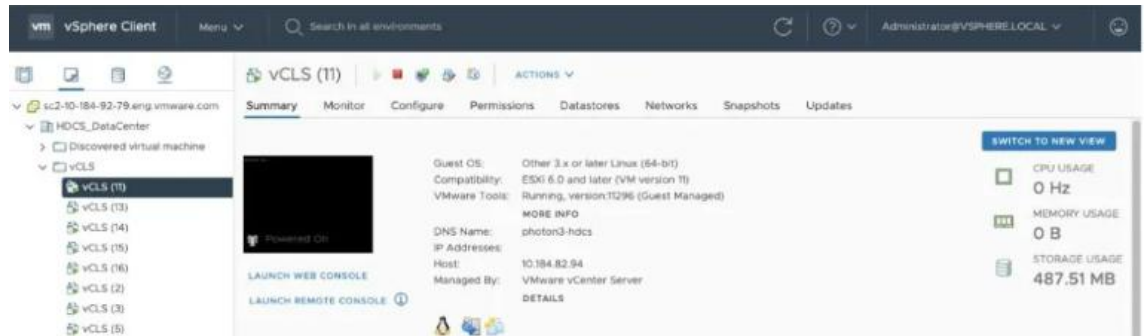


Figura 33. Administración de VMs desde vCenter Server. Recuperada de (VMware, 2022)

4.4.4 Crear Datacenter

Una vez finalizado el VCSA, ya se puede acceder para comenzar a configurar la estructura para administrar todos los nodos

Lo primero que se crea es un Data Center, que sería el contenedor principal de todo lo que tiene nuestro centro de datos, ya sean solo nodos o distintos cluster, como producción, test, preproducción, etc.

En vCenter, un Datacenter es un límite lógico para la jerarquía, mientras que un Cluster es un grupo de hosts ESXi gestionados conjuntamente para recursos compartidos (CPU, RAM, almacenamiento) que habilitan servicios avanzados como Alta Disponibilidad (HA) y Balanceo de Carga (DRS), ofreciendo tolerancia a fallos y eficiencia, a diferencia de hosts individuales (nodos) que están solos y gestionados por separado dentro del Datacenter.

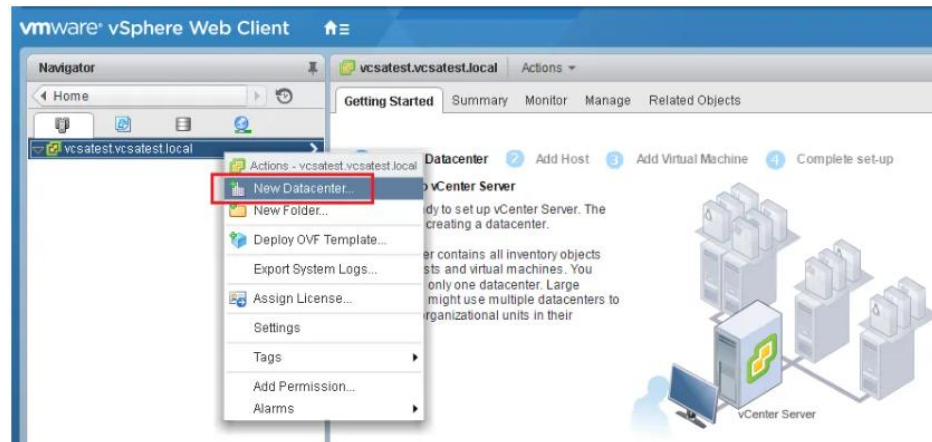


Figura 34. Panel para crear un Datacenter. Recuperada de (Nakivo, 2024)

4.4.4.1 Nodos Suetos (Hosts Individuales)

- **Gestión:** Cada servidor ESXi se añade directamente al Datacenter o a carpetas dentro de él, sin agruparse para recursos compartidos.
- **Funcionalidad:** No tienen HA ni DRS. Si un host falla, sus VMs se caen y deben reiniciarse manualmente en otro host.
- **Uso:** Ideal para laboratorios pequeños, hosts con requisitos muy específicos o cuando no se necesita tolerancia a fallos.

4.4.4.2 Nodos en un Cluster (Cluster de Hosts)

- **Gestión:** Varios hosts (nodos) se agrupan en un "Cluster" dentro del Datacenter para compartir recursos (CPU, RAM, almacenamiento).

- Funcionalidad: High Availability (HA) y Distributed Resource Scheduler (DRS)
- Uso: Entornos de producción donde la disponibilidad y la eficiencia son cruciales.

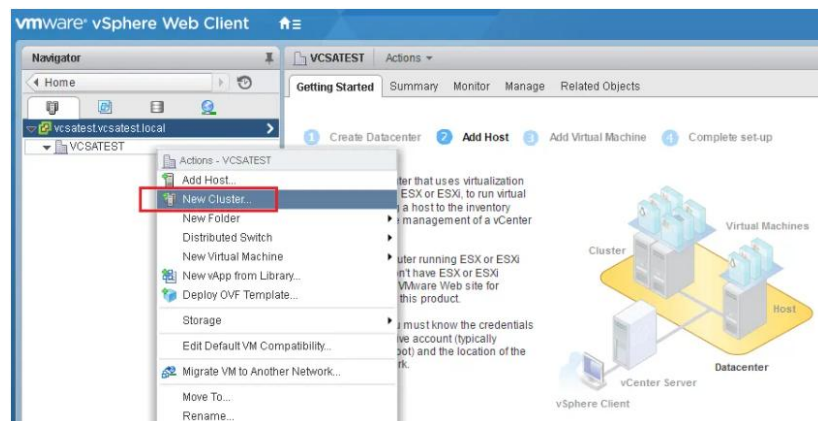


Figura 35. Panel para crear un nuevo Cluster. Recuperada de (Nakivo, 2024)

4.4.4.3 Añadir un nodo a vCenter

Para añadir un host ESXi a vCenter, inicia sesión en el cliente vSphere, haz clic derecho en el Centro de Datos o Carpeta donde quieres agregarlo, selecciona "Añadir Host", introduce la IP o nombre del host ESXi, proporciona las credenciales (usuario root y contraseña), acepta el certificado de seguridad y, opcionalmente, asigna una licencia y revisa la configuración antes de finalizar el asistente.

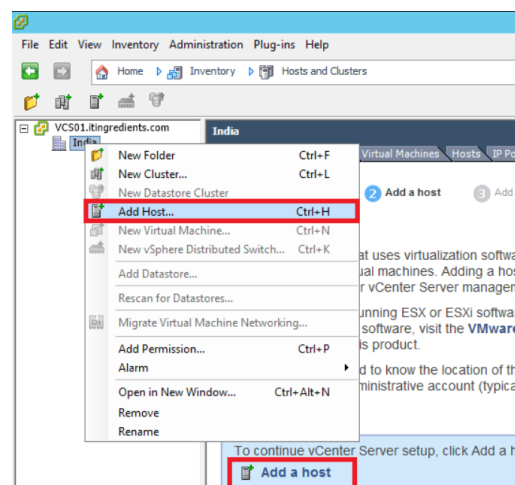


Figura 36. Panel para adherir un host. Recuperada de (Nakivo, 2024)

4.4.4.3.1 Pasos Detallados

Conéctate a vCenter: Abre tu navegador y ve a la URL de tu vCenter Server (https://<IP_o_Nombre_vCenter>/ui) e inicia sesión con tus credenciales de administrador.

Inicia el Asistente

- En la vista "Inventario" o "Hosts y Clústeres", haz clic derecho en el objeto donde quieres añadir el host (un Centro de Datos, una Carpeta, o un Clúster).
- Selecciona la opción "Añadir Host".
- Introduce los Detalles del Host:
- Nombre o IP: Escribe la dirección IP o el nombre de host del servidor ESXi que quieres agregar.

- **Credenciales:** Ingresa el nombre de usuario (generalmente root) y la contraseña del host ESXi.
- **Confirma la Conexión:** Puede aparecer una alerta de seguridad sobre el certificado del host ESXi. Confirma la conexión pulsando "Sí" para continuar, lo que reemplazará el certificado por uno emitido por vCenter.
- **Licencia y Resumen:** Asigna una licencia de ESXi si la tienes, o deja la de evaluación. Y Resumen, revisa la información del host y los ajustes propuestos.
- **Finaliza:** Haz clic en "Siguiete" y luego en "Finalizar" para completar el proceso. Las máquinas virtuales del host se agregarán automáticamente al inventario de vCenter.

vCenter: 192.168.101.103

hosts ESXi: 192.168.101.205, 192.168.101.207, 192.168.101.208

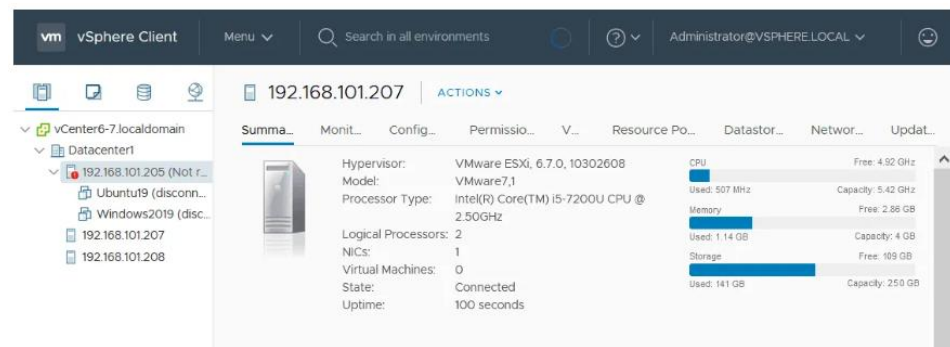


Figura 37. Vista de la consola VCSA con Data Center, cluster, y host con VMs. Recuperada de (Nakivo, 2024)

4.4.5 Creación de Cluster

En informática, un cluster es grupo de computadoras (nodos) interconectadas que trabajan juntas como un sistema único y unificado para lograr un objetivo común, ya sea para aumentar la potencia de procesamiento (computación de alto rendimiento, HPC) o para ofrecer alta disponibilidad y tolerancia a fallos. Estas máquinas, que pueden ser servidores, estaciones de trabajo o PCs, se comunican a través de una red y se gestionan como un solo recurso, permitiendo ejecutar tareas en paralelo y distribuir la carga de trabajo para mejorar el rendimiento y la fiabilidad.

Para crear un nuevo objeto de clúster de vSphere, utilice vSphere Client. Antes de comenzar debe tener en cuenta

- Compruebe que en el inventario hay un centro de datos o una carpeta dentro de un centro de datos.
- Compruebe que los hosts que integrarán el cluster tengan la misma versión de ESXi y el mismo nivel de revisiones.
- Obtenga el nombre de usuario y la contraseña de la cuenta de usuario raíz para el host.

Host > Inventario > Crear clúster

1. En la página de inicio de vSphere Client, vaya a Inicio > Hosts y clústeres.
2. Seleccione un centro de datos.
3. Haga clic con el botón derecho en el centro de datos y seleccione Clúster nuevo.
4. Introduzca un nombre para el clúster.
5. Seleccione las funciones de los clústeres de DRS, vSphere HA o vSAN.

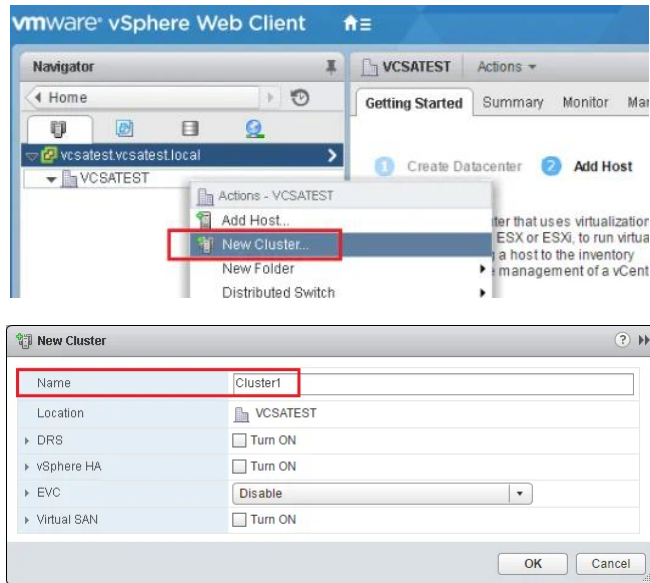


Figura 38. Configuración de un nuevo cluster desde la consola web de VCSA. Recuperada de (Nakivo, 2024)

Agregar hosts al cluster

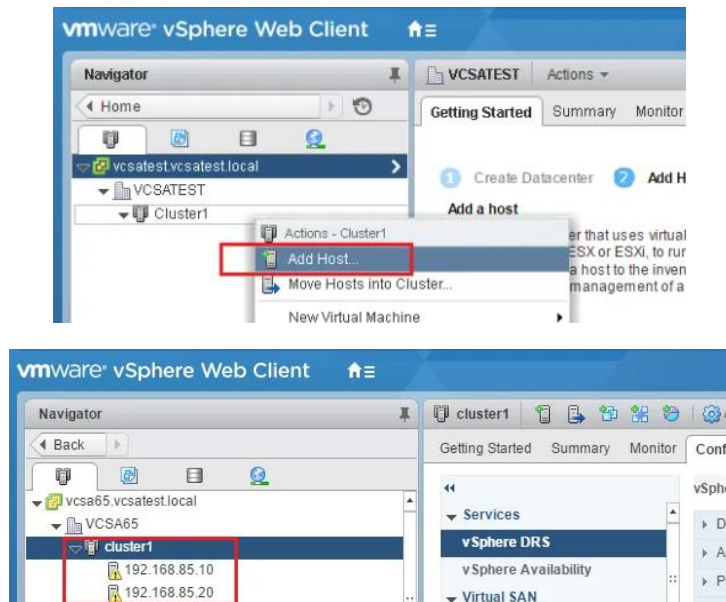


Figura 39. Agregar un nuevo host dentro de un cluster. Recuperada de (Nakivo, 2024)

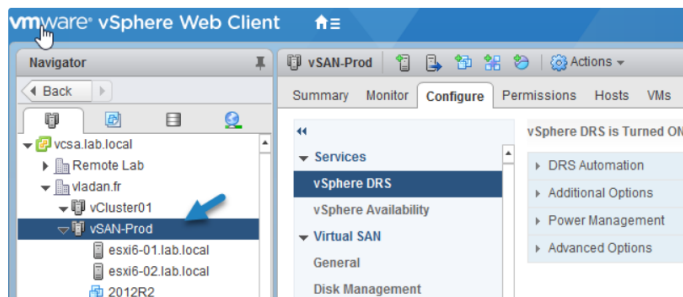


Figura 40. Vista de los hosts dentro un cluster. Recuperada de (Nakivo, 2024)

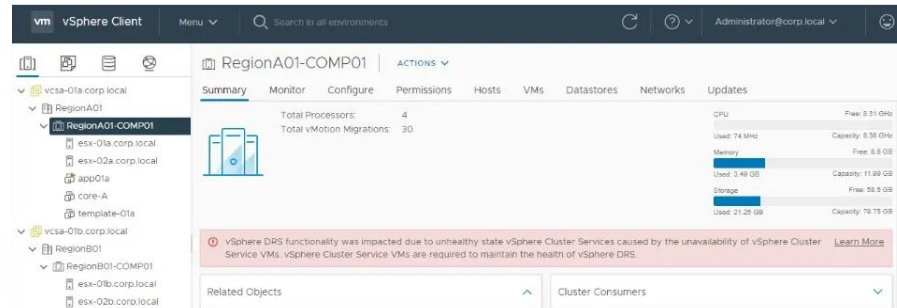


Figura 41. Vista general de la consola web un VCSA. Recuperada de (Nakivo, 2024)

En la configuración de clúster con el servidor VMware vCenter permite utilizar el centro de datos de la empresa Tecnologías VMware vSphere, como HA (alta disponibilidad) y DRS (programador de recursos distribuidos). Ambas tecnologías contribuyen a la tolerancia del clúster de VMware de soportar fallas, así como a la distribución de recursos entre los hosts de VMware ESXi. En la configuración de VMware ESXi independiente, esto no es posible [20].

4.5 Almacenamiento en vSphere vCenter

Al Comienzo de este capítulo se mencionaron los tipos de almacenamientos que son compatibles con vSphere vCenter. Pero es importante tener en cuenta que hay Datastores que no permite aplicar las principales funciones de alta disponibilidad en un cluster, y otros que si.

4.5.1 Datastores no compartidos

Los datastores que no permiten vMotion, HA y DRS son principalmente aquellos que no son compartidos, es decir, el almacenamiento local de cada host ESXi (Direct-Attached Storage - DAS), como discos duros internos, SATA, SAS o SSD locales. Al no ser accesibles por otros hosts, las funciones de alta disponibilidad y migración en caliente no operan.

- Datastores Locales (Local VMFS/VFFS): Son discos internos de un solo host ESXi. No permiten el movimiento de máquinas virtuales (VMs) en caliente (vMotion) ni el reinicio automático en caso de fallo (HA).
- Datastores en ESXi Free (Licencia Gratuita): Independientemente del tipo de almacenamiento, si el host ESXi usa la licencia gratuita, las funciones de vCenter como vMotion, DRS y HA no están disponibles.
- Dispositivos de paso directo (Passthrough/RDM Físico): Si un disco se mapea directamente a una VM en modo RDM físico, esto puede impedir vMotion, aunque no sea un tipo de datastore en sí mismo, sino una configuración de almacenamiento.

4.5.2 Datastores compartidos

Los datastores que sí permiten vMotion, HA y DRS son aquellos compartidos, como VMFS (en FC/iSCSI), NFS y vVOLs, ya que permiten acceso simultáneo a múltiples hosts.

Datastores que si permiten vMotion, HA y DRS: VMFS (Virtual Machine File System), NFS (Network File System), vVOLs (Virtual Volumes) y vSAN:

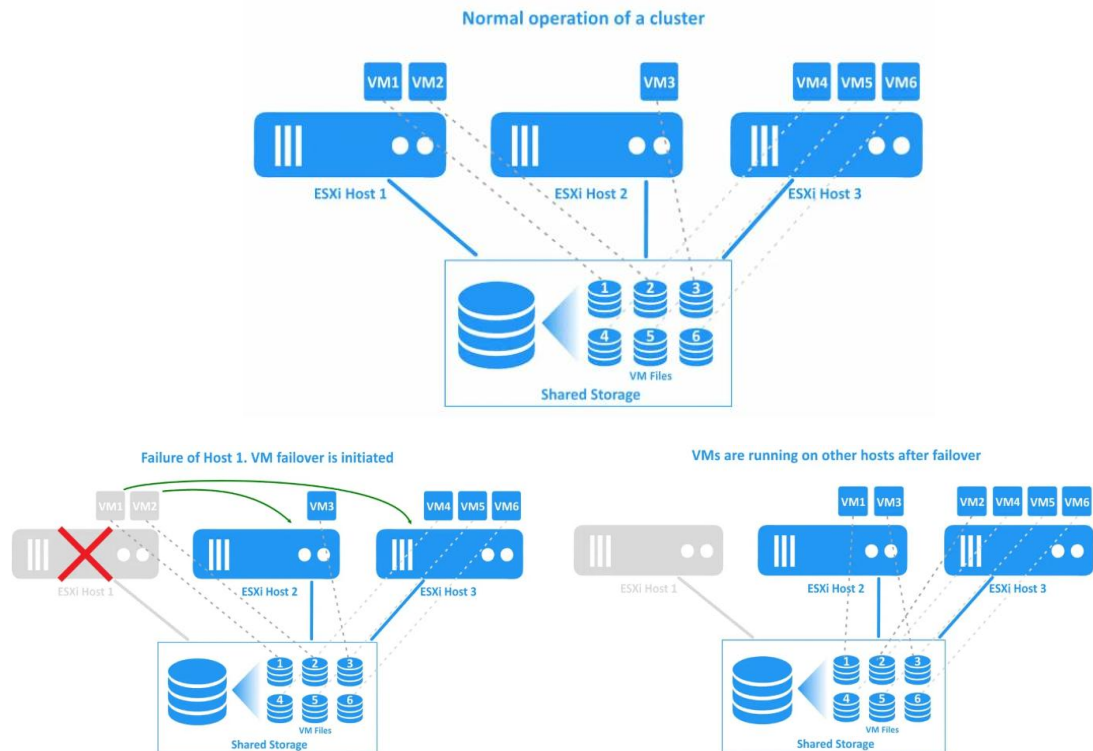


Figura 42. Funcionamiento de la Alta Disponibilidad en VMware vSphere vCenter.
Recuperada de (Nakivo, 2024)

4.5.3 Agregar un Datastore a vCenter

Para agregar un nuevo datastore VPLEX en vCenter, presente primero el volumen (LUN) desde la consola de administración de VPLEX a los hosts ESXi. Luego, en vSphere Client, vaya al host/clúster, seleccione Acciones > Almacenamiento > Nuevo almacén de datos, elija VMFS, seleccione el dispositivo VPLEX, asigne un nombre, y finalice el asistente.

1. Presentación de Almacenamiento (VPLEX): Asegúrese de que el volumen VPLEX esté enmascarado (zoned/masked) para los initiators WWPN de todos los hosts ESXi en el clúster.
2. Rescan de Almacenamiento (vCenter 8): En vSphere Client, haga clic derecho en el clúster o host > Almacenamiento (Storage) > Volver a examinar el almacenamiento (Rescan storage). Asegúrese de marcar las opciones para buscar nuevos dispositivos.
3. Crear el Datastore:
 - Clic derecho sobre el DataCenter, Clúster o Host donde se montará.
 - Seleccione Almacenamiento > Nuevo almacén de datos (New Datastore).
 - Seleccione VMFS como tipo de datastore.
 - Asigne un nombre al datastore y seleccione el dispositivo VPLEX de la lista de discos disponibles.
 - Seleccione la versión de VMFS (se recomienda VMFS 6 para vSphere 8).
 - Finalice el asistente con la configuración predeterminada de particiones.

Una vez completado, el nuevo datastore VPLEX debería estar visible bajo la pestaña "Datastores" y montado en todos los hosts necesarios para alta disponibilidad.

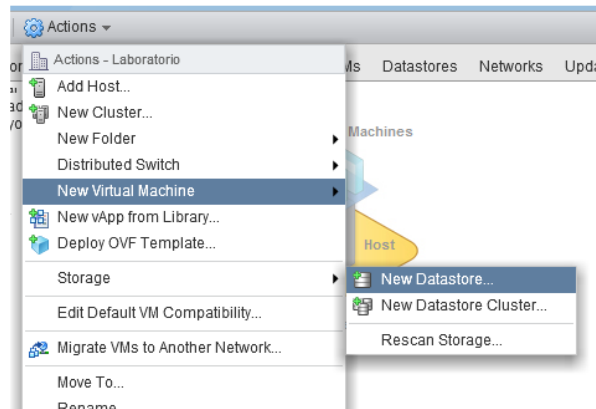


Figura 43. Agregar un nuevo Datastore al vCenter. Recuperada de (BlogVirtualizado, 2020)

Resumiendo, este capítulo trató sobre todo lo necesario para implementar un Data Center Virtual con administración centralizada y con cluster, para aprovechar las principales ventajas de vSphere: HA, DRS y FT. Se tuvo en cuenta todo lo necesario para implementar un Data Center de este tipo, teniendo en cuenta las características de hardware, software, almacenamiento y conexión.

El próximo capítulo explicará las herramientas y características de administrar un Centro de Dato con vCenter, que son las grandes ventajas que tiene este tipo de estructuras.

CAPÍTULO 5

Herramientas que potencian el uso de VMWare vSphere vCenter

5.1 Introducción

En este capítulo se tratarán las distintas herramientas que brinda vSphere vCenter, y por lo que hace la opción más elegida a nivel global para administrar Data Centers gestionando server físicos y virtuales de manera centralizada.

5.2 Herramientas Nativas de vCenter (Integradas en vSphere)

5.2.1 vMotion

vMotion es un tipo de migración de máquinas virtuales entre host mientras la máquina virtual está en funcionamiento, por lo que no es necesario apagarla ni suspender el sistema operativo. Se puede considerar una migración en vivo, lo que significa que no hay tiempo de inactividad ni interrupciones para los usuarios del sistema operativo durante la migración de la carga de trabajo.

Si VMware vMotion fallara, la máquina virtual simplemente volvería al host de origen.

vMotion no permite migrar máquinas virtuales entre vCenters [21].

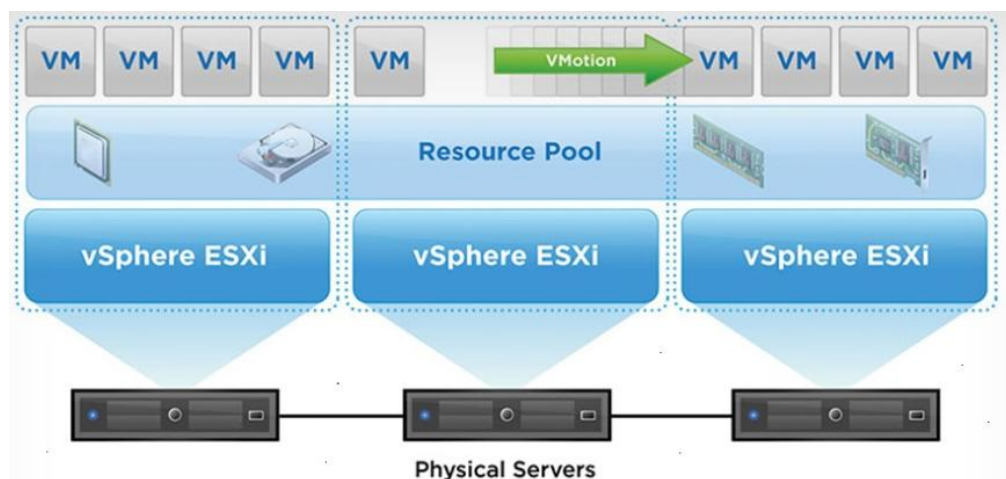


Figura 44. Funcionamiento de VMware vMotion. Recuperada de (Stephen Wagner, 2022)

5.2.1.1 Casos de uso de vMotion

Es muy útil cuando detecta un fallo en un servidor o este notifica una alerta, puede usar vMotion para migrar las máquinas virtuales de un servidor a otro sin apagarlas.

Si los recursos de hardware de un host determinado se consumen seriamente y hay otro host que está relativamente vacío, vMotion podría ayudarlo a migrar máquinas virtuales del host ocupado a otro host sin detener el sistema empresarial.

El servidor podría funcionar de forma continua durante mucho tiempo, pero el hardware aún necesita mantenimiento. Con vMotion, no habrá tiempos de inactividad ni se perderá la conexión a internet.

La función avanzada DRS (Programador dinámico de recursos) se puede ejecutar con vMotion para lograr un equilibrio de carga automático.

5.2.1.2 Como funciona vMotion

vMotion funciona migrando una máquina virtual (VM) en vivo de un host ESXi a otro dentro de un clúster vCenter, sin interrupción del servicio, copiando su estado (CPU, memoria) a través de una red de alta velocidad mientras mantiene la conectividad de red y el almacenamiento compartido. El proceso implica copiar la memoria activa, sincronizar los cambios y, finalmente, cambiar rápidamente el puntero de la VM al nuevo host, lo que permite mantenimiento o balanceo de carga sin tiempo de inactividad.

Paso a paso

Pre-migración y preparación

- Se configura una red dedicada de alta velocidad para vMotion en cada host ESXi.
- vCenter prepara el host de destino preasignando recursos y creando una versión "enmascarada" de la VM.
- Se inicia la copia de la memoria activa (páginas de RAM) del host de origen al host de destino.

Sincronización de memoria (Convergencia)

- vMotion rastrea las páginas de memoria que cambian (páginas sucias) y las replica continuamente en ciclos iterativos.
- Utiliza técnicas como "Stun While Page Send" (SDPS) si es necesario, para pausar brevemente la VM (microsegundos) y asegurar que toda la memoria se sincronice sin pérdida de datos.

Punto de corte (Cutover)

- Una vez que la memoria está casi completamente sincronizada, la VM de origen se "congela" por una fracción de segundo (el stun time).
- Se copian los últimos datos de memoria y los registros de la CPU.
- La VM se "descongela" y se inicia en el host de destino, manteniendo su identidad de red (MAC, IP).

Post-migración

- El almacenamiento compartido (SAN/NAS) permite que ambos hosts accedan a los archivos de disco de la VM, por lo que no se migran los discos durante vMotion, solo el estado de ejecución.
- La VM continúa funcionando en el nuevo host sin que el usuario note la migración.

Requisitos clave en un clúster

- **Almacenamiento Compartido:** Todos los hosts deben tener acceso al mismo almacenamiento (SAN/NAS) para que la VM pueda acceder a sus archivos de disco desde cualquier host.

- **Red Dedicada:** Se recomienda una red de alto rendimiento (10GbE o superior) para el tráfico de vMotion.
- **vCenter:** Orquesta el proceso de migración entre los hosts del clúster.
- **DRS (Distributed Resource Scheduler):** Puede mover VMs automáticamente entre hosts para balancear la carga dentro del clúster usando vMotion.

5.2.2 Storage vMotion

VMware Storage vMotion funciona copiando los archivos de disco de una máquina virtual (VM) en ejecución de un almacenamiento (datastore) a otro, sin interrumpir su servicio, mediante una migración en caliente que mantiene la VM activa mientras se mueven sus datos, lo que permite mantenimiento de almacenamiento, optimización de rendimiento y equilibrio de carga sin tiempo de inactividad, siendo una migración de datos sin afectar el host físico.

vMotion mueve la VM entre hosts físicos (CPU y memoria), manteniendo el almacenamiento igual. Mientras que Storage vMotion (SvMotion) mueve la VM entre datastores (almacenamiento), pero la VM sigue en el mismo host físico.

5.2.2.1 Cómo Funciona (Paso a Paso)

1. **Inicio de la Migración:** Se selecciona la VM y el nuevo datastore de destino a través de vCenter o vSphere Client.
2. **Copia de Datos:** Los archivos de disco virtual (VMDK) de la VM se copian del almacenamiento original al destino. Durante esta fase, cualquier escritura en el disco se realiza en ambos almacenamientos (origen y destino) para mantener la sincronización.
3. **Máquina Sombra:** Se crea una "máquina virtual sombra" en el nuevo datastore que empieza a apuntar a los discos en el destino.
4. **Pausa y Reanudación (Casi Instantánea):** La VM original se suspende por un instante imperceptible (milisegundos) y la ejecución se reanuda en la máquina sombra, que ahora lee y escribe desde el nuevo almacenamiento.
5. **Finalización:** Los archivos en el datastore original se eliminan, y la VM opera completamente en la nueva ubicación de almacenamiento.

Durante la migración de Datastore, si en la VM hay una operación de escritura, la misma se realiza en los discos del datastore de origen, como el datastore de destino. Hasta que no esté en los dos copiados, vmware no confirma al SO de esa VM el OK de escritura

Durante la migración, la VM que está cambiando sus discos de datastore, crea automáticamente una VM sombra. Esto se hace solo a nivel de recurso informático. Esa **VM sombra (shadow)** es una duplicación exacta de la VM, pero solo apuntando a los discos en el nuevo datastore. Cuando la migración se termina, la VM original se suspende, y la VM shadow arranca pasando a ser la original. Esto sucede en milisegundos, por eso para el usuario de este server es imperceptible.

5.2.2.2 Beneficios Principales

- **Mantenimiento Cero Downtime:** Realiza mantenimiento, actualizaciones o reconfiguraciones de almacenamiento sin apagar las VM.
- **Optimización de Almacenamiento:** Mueve cargas de trabajo a diferentes tipos de almacenamiento (ej. SSD vs. HDD) para equilibrar rendimiento y costos.
- **Flexibilidad:** Permite cambiar el tipo de aprovisionamiento (grueso a fino) o mover archivos de VM a ubicaciones específicas.

vMotion nos ayuda mucho a planificar el mantenimiento de hardware, para administrar mejor el almacenamiento, para optimizar el uso del almacenamiento, para aumentar los recursos sin mucha intervención. Colabora con una Buena Escalabilidad.

Un gran beneficio es planificar cuando moverlas de acuerdo a las necesidades del negocio. Hay servidores que durante todo un mes funcionan de manera normal, pero uno o dos días al mes se corren procesos que requieren muchos recursos y tiempo. Durante ese tiempo podés moverlos a un repositorio cuyos discos tengan mayor velocidad

5.2.3 DRS – Programador de Recursos Distribuidos

VMware DRS (Distributed Resource Scheduler) es una herramienta poderosa dentro de vCenter, que juega un papel fundamental en la optimización y gestión de la infraestructura virtual. Al analizar continuamente el uso de recursos como CPU, memoria y almacenamiento, DRS toma decisiones inteligentes sobre dónde colocar las máquinas virtuales para garantizar un rendimiento óptimo y una alta disponibilidad. Funciona como un equilibrador de carga automático dentro de un clúster de vSphere. Utiliza vMotion para migrar máquinas virtuales (VMs) y así conseguir equilibrar las cargas de trabajo, asegurando un uso óptimo de los recursos

5.2.3.1 Cómo funciona DRS

Monitoreo Continuo: DRS analiza cada 5 minutos (por defecto) el uso de CPU y RAM de todos los hosts y VMs en el clúster, calculando la demanda de recursos.

Cálculo de Demanda: Estima la demanda de CPU y memoria de cada VM usando datos históricos y actuales para predecir tendencias de consumo.

Detección de Desequilibrio: Si detecta que un host está sobrecargado o que una VM necesita más recursos (o menos), determina si es necesario un movimiento, y en caso de conformarlo, también selecciona la mejor ubicación.

Migración con vMotion: Utiliza vMotion para mover VMs entre hosts, equilibrando la carga de trabajo de forma transparente para el usuario y las aplicaciones.

Control de Agresividad: Permite ajustar un "umbral de migración" (de conservador a agresivo) para controlar la frecuencia de las migraciones, optimizando estabilidad o equilibrio.

Pools de Recursos: Se pueden crear "pools de recursos" para asignar prioridades y límites de recursos a grupos específicos de VMs, gestionando así de forma flexible la asignación (ej. VMs de desarrollo vs. producción).

Balance de carga: Distribuye la carga de trabajo de manera uniforme entre los hosts.

DRS es una función clave para la optimización dinámica de recursos, que, junto con VMware HA (High Availability), garantiza no solo la disponibilidad, sino también el rendimiento eficiente de las cargas de trabajo en un entorno virtualizado [22].

5.2.4 High Availability (HA) – Alta Disponibilidad

VMware High Availability (HA) es una función que proporciona una disponibilidad óptima para las máquinas virtuales vSphere, incluidas las aplicaciones y los servicios que se ejecutan en las máquinas virtuales, para minimizar el tiempo de inactividad en caso de fallos. La alta disponibilidad (HA), o la capacidad de un entorno virtual para soportar fallos de host, es una de las razones importantes por las que elige implementar VMware vCenter y un clúster en lugar de un host VMware ESXi independiente.

Cuando se ejecuta HA en un clúster VMware, se instala un agente en cada host que participa en el clúster. Cada agente de host se comunica con el otro y supervisa la accesibilidad de los hosts del clúster mediante heartbeats. Si transcurre un intervalo de 15 segundos sin que se reciban latidos de un host concreto y los pings al host también fallan, el host se declara fallido. Las máquinas virtuales que se ejecutan en los recursos de computación/memoria de ese host fallido se transfieren a un host sano y se reinician en ese host.

La HA en vSphere puede supervisar el estado del hardware de los hosts para retirar de forma proactiva las máquinas virtuales de los hosts con problemas de hardware. También hay prioridades de reinicio y orquestación incorporadas en HA y, como resultado, las máquinas virtuales designadas se ponen en línea antes que otras en caso de conmutación por error. Estas funciones están disponibles en las versiones VMware vSphere 6.7 y vSphere 7.

VMware HA permite minimizar el tiempo de inactividad de las máquinas virtuales en caso de fallo del host hipervisor (ESXi).

5.2.4.1 Diferencia entre DRS y HA en VSphere

DRS funciona para garantizar que las cargas de trabajo obtengan los recursos a los que tienen derecho mediante la ubicación o el equilibrio. vSphere HA garantiza la disponibilidad de la carga de trabajo cuando un host en un clúster falla, queda aislado o cuando se interrumpe el latido de una máquina virtual

5.2.4.2 Requisitos del clúster VMware con HA

Para crear un clúster de VMware vSphere con Alta Disponibilidad, los requisitos fundamentales incluyen un vCenter Server activo, al menos dos hosts ESXi (se recomiendan 3 o más) con licencias vSphere compatibles (Standard o Enterprise Plus), almacenamiento compartido (SAN/NAS/vSAN) y redes de gestión comunes. Los hosts deben tener direcciones IP estáticas y configuraciones de red homogéneas.

5.2.4.3 VMware vSphere HA proactiva

La HA proactiva es una función que hace que un clúster reaccione ante un problema antes de que se produzca un fallo en todos los hosts ESXi y las máquinas virtuales que residen en ese host. Los problemas pueden producirse con distintos componentes de un servidor ESXi, y vSphere Proactive HA puede detectar las condiciones de hardware de un servidor.

Por ejemplo, se puede notificar a HA proactiva que hay problemas con la fuente de alimentación de un servidor ESXi. Las máquinas virtuales siguen funcionando en este servidor, pero este problema puede provocar pronto un fallo del servidor. Para evitar posibles fallos de las máquinas virtuales, vSphere Proactive HA puede iniciar la migración de las máquinas virtuales a otros hosts ESXi de un clúster. La HA proactiva permite reaccionar ante problemas relacionados con la fuente de alimentación, el ventilador, el almacenamiento, la memoria y la red [23].

5.2.5 Fault Tolerance (FT):

Es una tecnología que proporciona disponibilidad continua para VMs críticas, creando una réplica exacta en vivo (sombra) en otro host, que se mantiene sincronizada y puede tomar el control instantáneamente si la VM principal falla, logrando una pérdida de datos y tiempo de inactividad casi nulos. Funciona replicando continuamente el estado de la VM principal a la secundaria usando la tecnología vLockstep, manteniendo ambas idénticas y preparadas para un cambio (failover) transparente y automático, sin interrumpir la aplicación.

5.2.5.1 Cómo funciona.

Creación de Réplica: Al activar FT en una VM, vCenter crea una "máquina virtual secundaria" idéntica en un host diferente del clúster, estableciendo una copia en vivo.

Sincronización Continua (vLockstep): Utiliza la tecnología vLockstep para replicar el estado de la VM principal (incluyendo instrucciones de CPU, memoria y estado de red) a la secundaria en tiempo real. Esto asegura que ambas VMs estén en el mismo punto exacto.

Redundancia de Almacenamiento: Mantiene dos copias de los archivos de la VM (discos, configuración) en almacenamiento compartido para tolerar fallas a nivel de disco.

Detección de Fallos: Si el host de la VM principal falla (falla de hardware completa), la VM secundaria toma el control automáticamente.

Failover Transparente: La VM secundaria se convierte en la principal, continuando el procesamiento sin interrupción, y vCenter inicia una nueva VM secundaria en otro host para restaurar la protección.

Requisitos Clave: Necesita un clúster con hosts compatibles (misma familia de CPU), almacenamiento compartido, una red de alta velocidad (idealmente 10 Gbps) para la replicación y VMs con un número limitado de vCPU (2-8, según la versión).

5.2.5.2 Diferencia con VMware HA (Alta Disponibilidad)

FT es una protección de nivel de aplicación con cero tiempo de inactividad y sin pérdida de datos, manteniendo una réplica activa todo el tiempo. Y HA protege al nivel de host; si un host falla, reinicia las VMs en otro host disponible, lo que puede generar una breve interrupción.

5.2.5.3 Limitaciones claves para decidir su uso

Antes de aplicarlo, se debe considerar que FT impone restricciones técnicas estrictas:

Consumo de recursos: Duplica el uso de CPU y RAM, ya que mantiene una "VM secundaria" idéntica ejecutándose en paralelo en otro host.

Escalabilidad: Está limitado a un máximo de 8 vCPUs y 128 GB de RAM (dependiendo de la edición de la licencia, como vSphere Enterprise Plus).

Incompatibilidad: No es compatible con snapshots de VM, dispositivos USB, ni RDMS físicos.

Compatibilidad con CPU del host: Deben ser compatibles con vSphere vMotion. Por ejemplo Intel Sandy Bridge y AMD Bulldozer o posterior.

Red: Usar una de registro de 10 Gbit para FT y verificar que la red tenga baja latencia. Se recomienda contar con una red de FT dedicada.

Cantidad máxima de VMs permitidas: Se permiten en un host en el clúster un valor predeterminado es 4.

Cantidad máxima de vCPU permitidas: Entre todas las VMs con Fault Tolerance en un host, el valor predeterminado es 8 [24].

5.2.6 VMware Tools

VMware Tools es un conjunto de controladores, servicios y módulos que se instalan directamente en el sistema operativo invitado (Guest OS) de una máquina virtual creada con productos VMware. Actúa como un puente de comunicación entre el sistema operativo invitado y el software de virtualización de VMware (el hipervisor).

VMware Tools permite la sincronización de la hora entre el host y el invitado y mejora la experiencia del usuario al ofrecer un mejor rendimiento del mouse (sin lag), un mejor rendimiento gráfico, un portapapeles compartido, la posibilidad de arrastrar & soltar archivos, secuencias de comandos para automatizar tareas dentro de una máquina virtual, entre otras.

Cuando se crea una máquina virtual, se debe seleccionar la versión de hardware. Las máquinas virtuales utilizan hardware emulado. Los controladores para este hardware emulado se instalan con VMware Tools. Una máquina virtual puede funcionar sin VMware Tools, pero se estará perdiendo la mayoría de las funciones y ventajas de usar máquinas virtuales. Se recomienda encarecidamente instalar VMware Tools en los sistemas operativos invitados que se ejecuten en máquinas virtuales VMware.

El conjunto de funciones disponibles después de instalar VMware Tools no es el mismo para diferentes sistemas operativos, por ejemplo, algunas funciones activadas para huéspedes Windows no están disponibles para huéspedes Linux [26].

5.2.6.1 Beneficios de instalar VMware Tools

La instalación de VMware Tools no es solo una recomendación; es prácticamente una necesidad para cualquier máquina virtual en producción o para una experiencia de usuario fluida. Sus beneficios incluyen:

Rendimiento mejorado: VMware Tools optimiza drásticamente el rendimiento de la máquina virtual al proporcionar controladores de alto rendimiento para componentes críticos como la red, el almacenamiento y los gráficos. Esto se traduce en un sistema operativo invitado mucho más rápido y responsivo, capaz de ejecutar aplicaciones de forma más eficiente y gestionar cargas de trabajo exigentes sin problemas.

Experiencia de usuario fluida: Este conjunto de utilidades habilita funcionalidades que mejoran significativamente la interacción con la máquina virtual. Permite el movimiento suave del ratón entre el sistema operativo host y el invitado sin necesidad de «capturarlo», facilita la copia y pegado bidireccional de texto e imágenes, y habilita la función de arrastrar y soltar archivos directamente entre el host y la VM, lo que hace el trabajo diario mucho más eficiente.

Gestión eficiente de la VM: VMware Tools proporciona al hipervisor una mejor comunicación con el sistema operativo invitado, lo que permite realizar operaciones de gestión importantes directamente desde VMware vSphere, Workstation o Fusion. Esto incluye la capacidad de realizar un apagado y reinicio limpio del sistema operativo, sincronizar la hora de la VM con la del host, y crear snapshots consistentes para máquinas virtuales con bases de datos o aplicaciones críticas, garantizando la integridad de los datos en las copias de seguridad.

Información y monitoreo detallado: Al instalar VMware Tools, el hipervisor recibe información detallada sobre el estado y el rendimiento del sistema operativo invitado. Esto es vital para el monitoreo del entorno virtual, permitiendo a los administradores observar métricas de uso de CPU, memoria y disco de la VM de forma más precisa. Además, facilita la asignación dinámica de recursos y la optimización general de la infraestructura virtual [26].

5.2.7 vCenter Server

vCenter proporciona un único punto de administración para todas las máquinas virtuales de su entorno. Este control centralizado simplifica tareas como el aprovisionamiento de nuevas VM, la configuración de sus parámetros, la supervisión de su rendimiento y la administración de sus ciclos de vida. Puede controlar sus hosts y máquinas virtuales desde una única consola, lo que mejora la visibilidad y ayuda a prevenir errores. El cliente vSphere basado en HTML 5 permite acceder a las funciones clave de vSphere desde cualquier navegador.

Permite a los administradores controlar múltiples servidores host ESXi y sus máquinas virtuales (VM) desde una única interfaz. Funciona como un "panel de control" para el centro de datos virtualizado, ofreciendo un control unificado y escalable sobre toda la infraestructura.

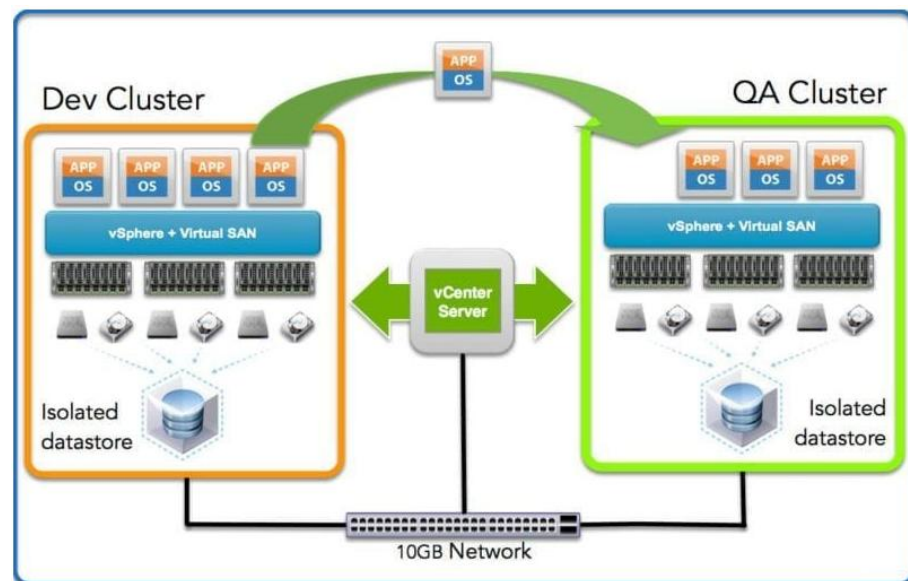


Figura 45. Estructura física administrada por vCenter.
Recuperada de (José María Gonzalez, 2019)

5.3 Herramientas de Gestión y Automatización Externas y/o Complementarias

5.3.1 PowerCLI

Es un conjunto de módulos PowerShell de VMware, que amplían las capacidades de PowerShell, para comprender comandos adicionales e interactuar con entornos VMware. Es una extensión de Microsoft PowerShell, y al instalar PowerCLI, se instalan comandos PowerShell específicos de VMware denominados commandlets (o cmdlets), que permite a los administradores gestionar y automatizar toda la infraestructura VMware desde la línea de comandos, usando cmdlets específicos con la sintaxis verbo-sustantivo, para tareas como aprovisionar, configurar, monitorizar y reportar, lo que ahorra tiempo automatizando tareas repetitivas.

Se conecta a vCenter con Connect-VIServer y ejecutando comandos como Get-VM, facilitando la creación de scripts para flujos de trabajo complejos.

Las últimas versiones de PowerShell, a diferencia de las anteriores, se distribuyen como módulos de PowerShell. Existen métodos online y offline para instalar PowerCLI en Windows [27].

5.3.1.1 Ventajas de trabajar con PowerCli

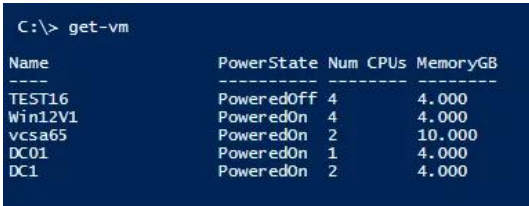
Ahorro de tiempo: Automatiza tareas tediosas y repetitivas.

Eficiencia: Permite obtener una visión rápida del entorno y administrarlo de forma eficiente.

Flexibilidad: Crea scripts reutilizables para configuraciones y despliegues.

Multiplataforma: Las versiones modernas funcionan en Windows, Linux y macOS.

Materiales disponibles: Hay muchos recursos excelentes en la web, incluidos sitios de blogs personales, documentación oficial, ejemplos de códigos, etc.. Se puede encontrar algo muy cercano a lo que se busca hacer, y con muy poca modificación adaptarlo a las nuevas necesidades.



```
C:\> get-vm
Name                PowerState Num CPUs MemoryGB
-----
TEST16              PoweredOff 4         4.000
Win12V1              PoweredOn  4         4.000
vcsa65               PoweredOn  2         10.000
DC01                 PoweredOn  1         4.000
DC1                  PoweredOn  2         4.000
```

Figura 46. Comando de PowerCli de VMware. Recuperada de (InfoWorld, 2023)

5.3.2 RVTools

Es una aplicación de Windows desarrollada en .NET que se utiliza para recopilar y mostrar información sobre máquinas virtuales y entornos virtuales en general. Esta herramienta utiliza el SDK de administración de VMware vSphere y la API REST de CIS para interactuar con VirtualCenter, ESX Server y otros componentes de VMware. Proporciona una amplia gama de información, incluyendo detalles sobre las VM, CPU, memoria, discos, particiones, redes, unidades de CD, dispositivos USB, instantáneas, herramientas de VMware, servidores vCenter, grupos de recursos, clústeres, hosts ESX, adaptadores HBA, tarjetas de red, conmutadores, puertos, consolas de servicio, núcleos de VM, almacenes de datos, información multipath, información de licencia y verificaciones de estado. RVTools ofrece una variedad de características y funcionalidades que lo convierten en una herramienta esencial para los administradores de sistemas.

Una de las principales fortalezas de RVTools es su capacidad para proporcionar información detallada sobre las máquinas virtuales. Puede mostrar detalles como el nombre de la VM, estado de energía, si es una plantilla, estado de configuración, nombre DNS, estado de conexión, estado del sistema operativo invitado, estado de latido, fecha y hora de encendido y suspensión, fecha y hora de creación, versión de cambio, número de CPU, sensibilidad a la latencia, cantidad de memoria, número de tarjetas de red, número de discos virtuales, capacidad total de disco, etc..

RVTools permite exportar la información recopilada en diferentes formatos, como archivos CSV y XLSX. Esto facilita el análisis y el uso de la información en otras herramientas y plataformas.

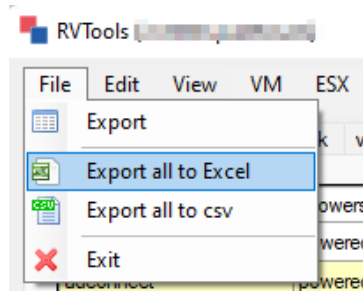


Figura 47. Exportar reporte de RVTools a Excel. Recuperada de (BlogVirtualizado, 2020)

RVTools es compatible con diferentes versiones de VMware, desde VirtualCenter 5.x en adelante. Esto garantiza que los administradores puedan utilizar RVTools independientemente de la versión de VMware que estén utilizando.

5.3.2.1 Principales beneficios de usar RVTools

Visibilidad y control: proporciona una visión detallada de los entornos virtuales, lo que permite a los administradores tener un control total sobre sus sistemas. La información recopilada por RVTools ayuda a identificar problemas, optimizar recursos y tomar decisiones informadas.

Ahorro de tiempo: Con RVTools, los administradores pueden obtener información detallada sobre sus entornos virtuales en un solo lugar. Esto ahorra tiempo al evitar la necesidad de recopilar información de diferentes herramientas y fuentes.

Optimización de recursos: Al conocer la configuración y el rendimiento de las máquinas virtuales, los administradores pueden optimizar los recursos para garantizar un uso eficiente y maximizar el rendimiento de los sistemas.

Solución de problemas y resolución de problemas: RVTools proporciona información detallada sobre las VM y los componentes del entorno virtual, lo que facilita la identificación y resolución de problemas. Los administradores pueden utilizar esta información para solucionar problemas de rendimiento, identificar cuellos de botella y mejorar la disponibilidad de los sistemas.

Planificación y capacidad: La información recopilada por RVTools también es útil para la planificación y capacidad de los entornos virtuales. Los administradores pueden utilizar esta información para estimar el crecimiento futuro, identificar la necesidad de recursos adicionales y tomar decisiones informadas sobre la expansión de los sistemas [28].

VM	Powerstate	Template	SRM Placeholder	Config status	DNS Name	Connection state	Guest state	Heartbeat	Consolidation Needed	PowerOn	Suspend t
vm-1000	poweredOn	False	False	green	vm-1000	connected	running	green	False	2023/06/03 07:01:56	
vm-1001	poweredOn	False	False	green	vm-1001	connected	running	green	False	2023/09/14 03:58:45	
vm-1002	poweredOn	False	False	green	vm-1002	connected	running	green	False	2023/09/27 16:31:08	
vm-1003	poweredOn	False	False	green	vm-1003	connected	running	green	False	2023/06/03 06:45:57	
vm-1004	poweredOn	False	False	green	vm-1004	connected	running	green	False	2023/06/03 06:45:58	
vm-1005	poweredOn	False	False	green	vm-1005	connected	running	green	False	2023/06/03 06:45:54	
vm-1006	poweredOn	False	False	green	vm-1006	connected	running	green	False	2023/06/03 07:03:57	
vm-1007	poweredOn	False	False	green	vm-1007	connected	running	green	False	2023/06/03 07:05:23	
vm-1008	poweredOn	False	False	green	vm-1008	connected	running	green	False	2023/09/23 03:44:27	
vm-1009	poweredOn	False	False	green	vm-1009	connected	running	green	False	2023/09/07 18:30:44	
vm-1010	poweredOn	False	False	green	vm-1010	connected	running	green	False	2023/09/13 04:12:38	

Figura 48. Reporte de RVTools. Recuperada de (BlogVirtualizado, 2020)

5.3.3 vCenter Converter

VMware vCenter Converter Standalone es una aplicación gratuita que se puede descargar desde el sitio web de VMware e instalarse en Windows para convertir los tipos de máquinas compatibles en máquinas virtuales VMware. Es decir que convierte servidores físicos (P2V) o máquinas virtuales de otras plataformas, como Hyper-V, Citrix XenServer; en máquinas virtuales compatibles con VMware (V2V), facilitando la migración, consolidación y modernización de infraestructuras de TI, haciendo la migración "en caliente" (P2V) o "en frío" (V2V). Una característica importante es que no requiere ser un administrador de vCenter para usarla en migraciones básicas,

El VMware vCenter Converter Standalone se llama Standalone porque puede instalarse en el sistema operativo de una máquina personalizada.

5.3.3.1 Componentes de VMware vCenter Converter Standalone

- **Converter Standalone Server** es el componente principal que gestiona todas las tareas de conversión y maneja las conexiones entre otros componentes.
- **Converter Standalone Agent** es el componente que permite convertir la máquina en la que está instalado el agente. Si instalas el agente en tu máquina local cuando instales VMware Converter, podrás convertir tu máquina física en una VM.
- **Converter Standalone Client** es el componente que le permite conectarse al VMware Converter Standalone Server remoto y gestionar las tareas de conversión en esa máquina remota. El cliente proporciona la interfaz gráfica de usuario de VMware Converter.

Puede seleccionar los componentes que desea instalar cuando ejecute el instalador de VMware Converter. Hay dos opciones disponibles:

- Instalación local. Los tres componentes se instalan en una máquina local (servidor, agente y cliente).
- Instalación cliente-servidor (avanzada). Puede seleccionar los componentes del conversor que desea instalar.

5.3.3.2 Migración en frío y en caliente

La **migración en caliente** es el proceso de conversión de una máquina que se encuentra en estado encendido. No se recomienda la migración en caliente para convertir controladores de dominio de Active Directory. Se recomienda encarecidamente detener todas las posibles aplicaciones y servicios que escriban datos en los discos antes de iniciar la migración en caliente.

La **migración en frío** es la migración de una máquina fuente que se encuentra en estado apagado. La migración en frío se recomienda para convertir servidores MS Exchange, servidores de bases de datos como Oracle o MS SQL, y otros servidores en los que los datos cambian dinámicamente cuando se enciende un servidor (para preservar la coherencia de los datos).

Si los datos de los discos permanecen estáticos, puede realizar una migración en caliente. La migración en frío de servidores físicos puede realizarse si se arranca desde el Live CD y se ejecuta el proceso de conversión de una máquina física, incluidas las unidades de disco y el sistema operativo.

5.3.4 MobaXterm/WinSCP

MobaXterm y WinSCP son herramientas excelentes para administrar hosts ESXi/vCenter: MobaXterm es una solución todo-en-uno que ofrece terminal (SSH), SFTP con arrastrar y soltar, RDP y más, integrando todo en una interfaz; mientras que WinSCP es un cliente SFTP/SCP/FTP dedicado, ideal para transferencias de archivos seguras y sencillas a estos sistemas virtuales, especialmente útil para cargar archivos grandes o configurar conexiones específicas. Ambos facilitan la transferencia y gestión de archivos y comandos, aunque MobaXterm combina más funciones en una sola aplicación.

5.3.5 ESXCLI

Es una potente herramienta de línea de comandos incluida en VMware vSphere para administrar hosts ESXi, permitiendo configurar almacenamiento, redes, hardware y usuarios de forma local o remota. Es fundamental para tareas avanzadas de administración del sistema, diagnóstico y automatización, sin depender de la GUI, funcionando tanto en entornos independientes como gestionados por vCenter. A diferencia de PowerCLI, que es un conjunto de módulos de PowerShell que extiende las capacidades de PowerShell para administrar VMs de VMware,

ESXCLI es una herramienta de scripting en Python para la administración de hosts ESXi a través de la línea de comandos (Shell de ESXi, SSH, vCLI).

5.3.5.1 Habilitar la consola ESXi Shell

Por defecto, ESXi shell está desactivado para el acceso local y remoto. Esto significa que no puede ejecutar comandos de shell ESXi hasta que habilite el shell ESXi o el acceso SSH. VMware impone esta restricción por motivos de seguridad.

Hay tres formas de habilitar la consola

- Utilizando la interfaz ESXi por defecto
- Usando la consola de VMware Host Client
- En la consola mediante vCenter y VMware vSphere Client [29]

5.3.6 vRealize Log Insight –VMware Area Operations for logs

vRealize Log Insight es un software que ofrece la mejor gestión de log en tiempo real, especialmente para entornos VMware, y cuenta con una interface HTML5 fácil de usar. Con vRealize Log Insight podremos centralizar todos los eventos de nuestra infraestructura VMware. Funciona como un colector y analizador de logs que facilita de manera rápida y mucho más eficiente la resolución de problemas de nuestra Infraestructura. Recibe información no procesada creada por equipos de la Infraestructura, y lo transforma en series de tiempo y eventos, de manera que los Administradores pueden buscar, agregar y visualizar colecciones de información para analizar y tener una visión más clara de su entorno.

Es un appliance virtual basado de Photon Linux. Se implementa descargando el archivo OVA del sitio oficial de VMWare. Actúa como un servidor syslog proporcionando varias vistas e información que podremos visualizar de los eventos extraídos de las configuraciones de VMware.

Por ejemplo, el tiempo que tomaría revisar los logs de manera individual en un clúster de 20 host ESXi, es muy grande. Sumado a poder interpretarlos de forma correcta y encontrar la cadena de sucesos o anomalía que produjo al problema. Es en situaciones como esta donde vRealize Log Insight aporta su gran potencial [30].

5.3.6.1 Funcionamiento de vRealize Log Insight

1. **Recopilación:** Agentes de Log Insight se instalan en máquinas Windows/Linux o se configuran en dispositivos para enviar datos de syslog (UDP/TCP/SSL) al servidor central.
2. **Centralización y Análisis:** Los logs se envían a una instancia centralizada (un dispositivo virtual) donde se procesan, analizan y se estructuran para su consulta.
3. **Visualización y Alertas:** Los datos se presentan en paneles (dashboards) personalizables, se buscan usando lenguaje natural y se configuran alertas para eventos específicos o críticos.

5.3.6.2 Características principales de Log Insight

- **Recopilación y Centralización:** Ingesta de logs desde múltiples fuentes (vSphere, Windows, Linux, aplicaciones) en un solo lugar.
- **Análisis en Tiempo Real:** Permite buscar, correlacionar eventos y analizar la causa raíz (RCA) rápidamente.
- **Dashboards Personalizables:** Paneles interactivos para visualizar métricas, eventos y tendencias de rendimiento.
- **Alertas y Notificaciones:** Creación de alertas personalizadas para eventos críticos o de cumplimiento, con notificaciones por email o integraciones.
- **Auditoría y Cumplimiento:** Funciones para monitorear la postura de cumplimiento y realizar auditorías de seguridad.
- **Búsqueda en Lenguaje Natural:** Interfaz intuitiva para buscar información en logs sin necesidad de sintaxis compleja.
- **Integración:** Se integra con vRealize Operations Manager (vROps) para correlacionar logs con eventos de rendimiento.

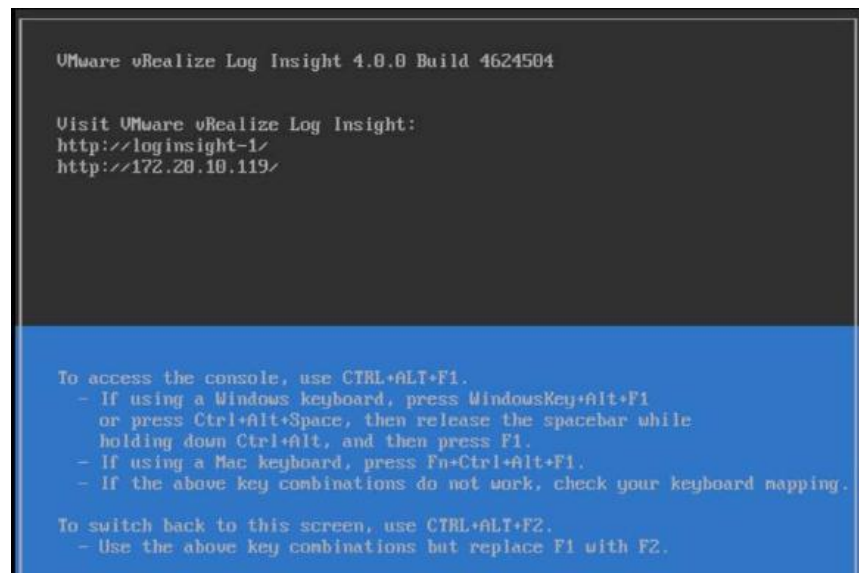


Figura 49. Consola VM de VMware vRealize Log Insight.
Recuperada de (Mohammed Raffic, 2017)

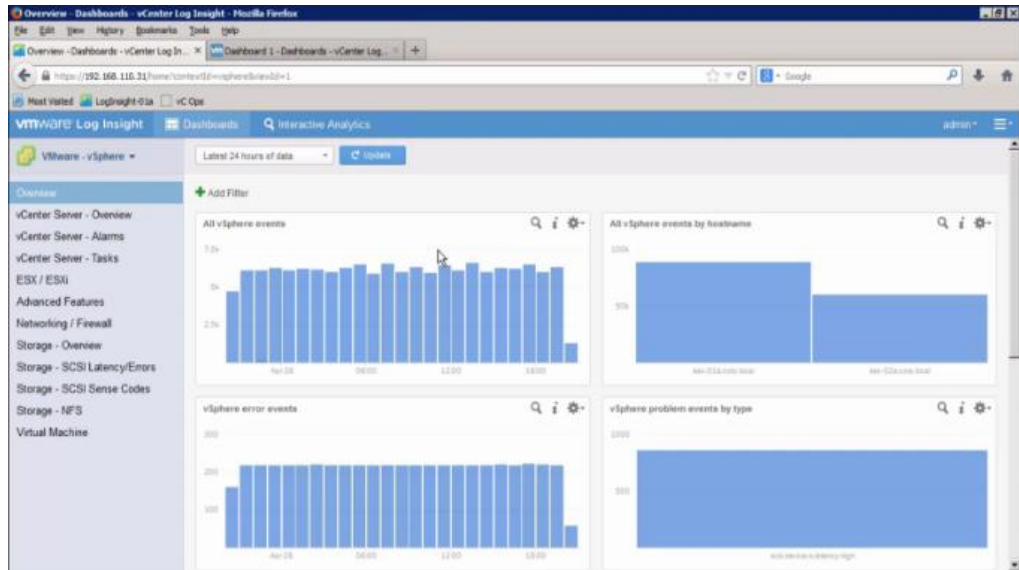


Figura 50. Dashboard VMware vRealize Log Insight.
Recuperada de (Jorge de la Cruz, 2015)

5.3.7 Herramientas de backup y replicación.

Los entornos VMware modernos se enfrentan a amenazas cada vez mayores que las instantáneas básicas y las herramientas nativas no siempre pueden abordar de manera adecuada. Los ataques de ransomware se dirigen cada vez más a la infraestructura virtualizada, ya que saben que comprometer las máquinas virtuales puede paralizar organizaciones enteras. Más allá de las amenazas externas, las organizaciones deben protegerse contra el borrado accidental, los fallos de hardware y la corrupción de datos, al tiempo que cumplen con los estrictos requisitos de cumplimiento normativo de sectores como el sanitario, el financiero y el gubernamental.

Las soluciones de copia de seguridad para empresas proporcionan la protección integral que exigen los entornos VMware: copias de seguridad coherentes con las aplicaciones que garantizan la integridad de las bases de datos y los servidores de correo electrónico, capacidades de recuperación granular que restauran archivos individuales sin recuperar máquinas virtuales completas y opciones flexibles de recuperación ante desastres, incluida la replicación entre sitios y la recuperación completa. Los marcos normativos como el RGPD, la HIPAA, el PCI-DSS y la SOX exigen medidas específicas de protección de datos, períodos de retención y registros de auditoría que las herramientas nativas de VMware por sí solas no pueden satisfacer.

La continuidad del negocio depende de la rápida recuperación ante cualquier situación de fallo. Ya sea ante el cifrado por ransomware, la eliminación accidental de máquinas virtuales, el fallo del sistema de almacenamiento o los desastres en el centro de datos, las organizaciones necesitan capacidades de copia de seguridad y recuperación probadas con objetivos de punto de recuperación (RPO) y objetivos de tiempo de recuperación (RTO) claramente definidos [31].

5.3.7.1 Principales soluciones de Backup y Replicación para VMware vCenter

Estas soluciones permiten la protección continua, réplica de máquinas virtuales (VMs) entre sitios y recuperación ante desastres (DR), integrándose directamente con la infraestructura VMware vSphere.

- **Veem Backup & Replication:** Solución integral líder para entornos virtuales, ofreciendo backups rápidos y replicación con soporte para inactividad casi nula.

- **NAKIVO Backup & Replication:** Especializada en entornos virtuales y cloud, permite replicar VMs en tiempo real y realizar copias de seguridad consistentes.
- **Zerto Virtual Replication:** Enfocada en la recuperación ante desastres (DR) y movilidad de cargas de trabajo con replicación continua basada en hipervisor.
- **VMware vSphere Replication:** Solución nativa de VMware que ofrece replicación asíncrona de máquinas virtuales, totalmente integrada en vCenter Server.
- **Rubrik / Cohesity:** Plataformas de gestión de datos modernas que agilizan la protección y automatización en infraestructuras definidas por software.

5.3.7.2 Dispositivos físicos de respaldo de alto rendimiento

Existen dispositivos físicos de almacenamiento de alto rendimiento y deduplicación diseñados para copias de seguridad rápidas en entornos VMware vSphere/vCenter. Estos sistemas se caracterizan por el uso de discos duros (HDD) de alta capacidad con tasas de transferencia rápidas, deduplicación de datos agresiva para maximizar la retención y una integración profunda con la API de VMware vStorage para respaldos sin agentes. Incluyen principalmente soluciones de almacenamiento definido por software (SDS) y matrices de respaldo dedicadas. Entre los más populares se encuentran

- **Dell PowerProtect Data Domain (DD Series):** Líder en deduplicación en línea, diseñado para integrarse con vCenter y software como Veeam o NetBackup.
- **ExaGrid Tiered Backup Storage (EX Series):** Ofrece una zona de aterrizaje (Landing Zone) de alto rendimiento para restauraciones inmediatas de máquinas virtuales y almacenamiento a largo plazo deduplicado.
- **HPE StoreOnce Systems:** Solución escalable con tecnología StoreOnce Catalyst, optimizada para copias de seguridad de entornos virtuales.
- **Veritas NetBackup Appliances:** Equipos llave en mano que combinan almacenamiento y software de respaldo, ideales para entornos vCenter complejos.
- **Quantum DXi Series:** Dispositivos de deduplicación de alto rendimiento que aceleran los respaldos de VMware.
- **Cohesity DataPlatform:** Plataforma hiperconvergente secundaria que ofrece respaldo, recuperación y gestión de datos nativa para vCenter.

5.3.7.3 Ventajas y Desventajas de aplicar backup y replica

El uso de soluciones de backup y replicación en vSphere (vCenter) garantiza la continuidad operativa mediante la protección de datos y alta disponibilidad, con tiempos de recuperación (RTO) y puntos de recuperación (RPO) mínimos. Las ventajas incluyen recuperación instantánea, inmutabilidad contra ransomware y replicación offsite, mientras que las desventajas se centran en el alto consumo de almacenamiento y recursos de red, además del tiempo de configuración.

CAPÍTULO 6

Mejoras en la administración de DataCenter, usando VMWare vCenter como Management principal

6.1 Introducción

En este capítulo trataremos las grandes mejoras que se obtuvieron al migrar a un Data Center Virtual Centralizado, con respecto al Data Center tradicional. Si bien la diferencia es abismal, pasar de un modelo a otro implica un gran trabajo, acompañado de una gran inversión. Hay que tener en cuenta que estas herramientas se usan en empresas grandes, con mucha cantidad de datos que se procesan sobre cientos de servidores, sumado a la alta disponibilidad necesaria de sus servicios.

Estas herramientas funcionan sobre una infraestructura integrada por equipos muy potentes y costosos, con un buen servicio de soporte y postventa y las licencias de estas herramientas son muy caras. Con gran inversión en conexiones LAN y SAN de alta velocidad. Requiere de la administración y soporte de un equipo interdisciplinario, con constante capacitación para potenciar las prestaciones del Data Center. Todo apuntando a mejorar la calidad del servicio de la organización. Por eso no siempre es viable adoptar esta implementación. La actividad de la empresa debe ser la principal justificación para determinar su uso.

Pero antes de ver las ventajas, trataremos un poco como es generalmente un escenario al encarar una migración de este tipo. Ver los distintos problemas que se pueden presentar, y como se fueron sorteando hasta lograr que el Data Center sea casi 100% virtual. Y se dice “casi”, porque hay varios servidores que, por sus características, se siguen manteniendo de la manera tradicional.

6.2 Migración al nuevo de Data Center – Análisis y planificación para la migración

El objetivo principal de la migración es lograr que toda la estructura del Data Center sea virtualizada y con gestión centralizada.

Planificar la migración a la nueva estructura administrada por vCenter desde un Data Center tradicional implica; evaluación, diseño, pruebas y ejecución por fases, priorizando la seguridad de los datos y minimizando el tiempo de inactividad. Es recomendable hacer un inventario detallado, definir objetivos, crear una hoja de ruta, ejecutar migraciones piloto, y finalizar con monitoreo post-migración.

Una vez finalizada la instalación de la nueva arquitectura física administrada por vCenter, con clusters, jerarquías de hosts, datastore y redes virtuales nuevas conviviendo con las ya existentes en las conexiones anteriores, se realiza como primera medida, un Inventario del Data Center a migrar, que documente servidores físicos, servidores virtuales, aplicaciones, dependencias, y requisitos de recursos (CPU, RAM, almacenamiento, red), etc.

6.2.1 Priorización.

Por cada servidor a migrar se debe tener en cuenta la carga de trabajo, horario sobre la disponibilidad, volumen de la información a procesar, vinculación con otros servers, Además

conocer los diversos sectores que deben intervenir en la migración, como DBA, SysAdmin, desarrolladores, seguridad, y los usuarios del sistema para realizar las pruebas necesarias post migración.

Teniendo en cuenta estos parámetros, entre otros, a cada server se le daba una ponderación de criticidad.

Como medida para agilizar el proceso de migración, se priorizó iniciar con aquellos servers que tuvieran menos carga de trabajo, sin necesidad de gran disponibilidad, y con la menor intervención de distintos sectores, es decir menor criticidad. Esto sirve, no solo para ir avanzando con la migración, sino también para tomar experiencias y tener en cuenta los nuevos inconvenientes que aparecían al momento de migrar y que en un comienzo no se tenían presente. En Data Center muy grandes, con gran variedad de sistemas, se presentaban escenarios muy diversos. Por lo que muchas veces se producía situaciones no deseadas y muy distintas a las planificadas.

En etapas más avanzadas se dejaron para migrar los servers más críticos, no solo por su importancia en el negocio, sino por su gran tamaño y complejidad para hacerlo, y con varios sectores que intervenían tanto en el proceso de migración como en las pruebas post migración. Las experiencias previas aportaban mucho agilizando un poco más las migraciones posteriores.

Finalizar con toda la migración llevo unos buenos años. Conviviendo las dos estructuras por un buen tiempo. En muchos casos, se aprovechó para que varios servidores se migraran por completo, realizando una implementación desde cero en la nueva estructura, con un SO más reciente, y herramientas más actuales. La complejidad de la migración fue mucho más engorrosa de lo esperado. Porque no solo se tiene que lidiar con lo asociado directamente a la migración en sí, sino también con los inconvenientes al tener que intervenir otras áreas, para pruebas, correcciones y en muchos casos reconfiguraciones.

6.2.2 Depuración de tecnología obsoleta y sistemas no utilizables

Varios servers críticos se tornaban muy complicado migrarlos, no solo por su tamaño, sino por su obsolescencia. Esta migración trajo el cumplimiento de nuevos objetivos que se habían planteado para más adelante, y es la de actualización de servidores a tecnologías más recientes. Específicamente a servidores con versiones más recientes de SO, SQL Server, Apache Tomcat, PHP, Java, ASP, FrameWork etc. En estos casos se creaba una VM en la nueva infraestructura, con el Sistema Operativo y las aplicaciones más recientes que estuviera homologado por la empresa proveedora. Se realizaba la configuración de las aplicaciones y servicios y todas las pruebas pertinentes. Una vez finalizado, se efectuaba la migración. Esto generaba un retrabajo extra, además con alto grado de dependencia de otros sectores y en la mayoría de los casos, de los proveedores. Esto provocaba una extensión considerable de la planificación original.

Durante la migración se evidenció que habían sistemas y servidores que ya dejaron de usarse y nunca se les dio de baja. En estos casos se les realizaba un backup para futuras recuperaciones y se les daba de baja. Colaborando así con la reducción del volumen de sistemas.

6.2.3 Agrupamiento de Sistemas por características y funcionalidades comunes.

Algunos servidores contaban con diversos servicios web, que no tenían nada que ver entre ellos. Esto también se trató de corregir en la migración. Luego de análisis se determinó la conveniencia de aislar servicios dejándolos en un servidor totalmente independientes. Y en otros casos agrupando algunos servicios de acuerdo a su funcionalidad o características comunes en sus herramientas. Pero se trataba de dejar servicios lo más aislado posible. El

criterio en estos casos es mantener una coherencia entre el servidor y sus servicios, facilitando la detección y corrección de incidentes. Antes de realizar esta etapa, ocuparse de solucionar los inconvenientes de algún servicio determinado, provocaba la interrupción de servicios ajenos, pero que convivían bajo la misma estructura y SO.

6.2.4 Inconvenientes para mantener la disponibilidad durante la migración

VMware Converter, la principal herramienta que se usó para migrar servidores a la nueva infraestructura, si bien trabaja online, es decir mientras el server está encendido, asegurando un constante servicio, en muchos casos no era posible trabajar de esa manera. Sobre todo en aquellos servers cuyos sistemas tenían una alta tasa de lectura/escritura, porque existe un alto porcentaje de generar inconsistencias. Para una fiel copia del server original, una buena práctica es realizarlo con el server original offline, es decir con sus sistemas o servicios de bases de datos totalmente detenidos, afectando directamente la disponibilidad de sus prestaciones.

Esto también influía considerablemente en la replanificación constante de la migración. La mayoría era fuera de horario laboral y en muchos casos priorizando los momentos de menor interacción de los servicios con los clientes. Tener en cuenta que algunos servers funcionaban sobre estructuras muy obsoletas y lentas, lo que provocaba que al momento de migrarlo con VMware converter aumentaba considerablemente la interrupción de la disponibilidad de los servicios

6.3 Ventajas de administrar un Data Center virtualizado y centralizado

6.3.1. Mantener distintos ambientes independientes.

Tener múltiples clústeres independientes dentro de un mismo vCenter ofrece mayor aislamiento, flexibilidad para separar cargas de trabajo (producción, desarrollo, distintas áreas de negocio) con políticas y recursos distintos, y mejora la resiliencia al limitar el impacto de fallos, mientras que la gestión centralizada de vCenter simplifica la supervisión general, aunque requiere una estrategia clara para la administración de permisos y la migración entre ellos.

Ventajas Clave

- **Aislamiento y Seguridad:** Separa entornos (ej., Dev, QA, Prod) para que un problema en uno no afecte a los demás, con políticas de seguridad y acceso distintas.
- **Gestión de Recursos Granular:** Permite asignar diferentes niveles de recursos (CPU, RAM, almacenamiento) y configurar funciones avanzadas (DRS, HA) de forma específica para cada clúster.
- **Flexibilidad y Escalabilidad:** Facilita la expansión de la infraestructura por fases o para diferentes departamentos, sin necesidad de grandes reestructuraciones.
- **Rendimiento y QoS:** Balancea la carga de trabajo de forma más eficiente dentro de cada clúster y puede priorizar aplicaciones críticas, mejorando la calidad de servicio (QoS).
- **Mantenimiento y Actualizaciones:** Permite realizar mantenimiento o actualizaciones en un clúster sin interrumpir los servicios en otros, con estrategias como vMotion para mover VMs entre hosts.
- **Gestión Centralizada (vCenter):** Un único punto para supervisar y administrar todos los clústeres, aunque pueden ser administrados de forma independiente, ideal para una visión global.

Existen otras maneras de tener en vCenter áreas de trabajo independientes (como entornos de Desarrollo, Pruebas, Producción) dentro del mismo clúster usando Carpetas (Folders) y

Resource Pools (Grupos de Recursos) para aislar grupos de VMs y controlar recursos. No es un aislamiento total, son solo ambientes lógicos y aislados dentro de un pool de recursos físicos compartido.

6.3.2 Ambiente de prueba idóneo.

Anteriormente el ambiente de prueba estaba sobre una estructura bastante precaria, Se reutilizaban servidores que eran reemplazados por su obsolescencia, con discos y tecnología que ya habían superado ampliamente su vida útil.

Era tan limitado, que solo algunos sistemas tenían su ambiente de prueba. Y lo más complicado es que el equipo de prueba era muy diferente en cuanto a características que el productivo. Por lo que muchas veces, las pruebas de nuevas implementaciones que se realizaban en test no aseguraba que funcionara en producción. Complicando aún más el pase a producción, lo que conllevaba a realizar rollback varias veces y demorar las nuevas implementaciones.

Otras implementaciones se realizaban directamente en producción, con el riesgo que ello conlleva

Además, era muy informal ese ambiente de pruebas. No había una figura como responsable para administrarlo. Se creaba un servidor con ciertas características destinado para testeo de un sistema en particular, y después se usaban ese mismo servidor para otras implementaciones, sin un mínimo criterio. Lo que conllevaba a que se perdiera el control de los servicios o sistemas que se encontraban en cada servidor. Si bien también se usaba vmware esxi para implementar servidores virtuales, eran versiones muy obsoletas y que no contaban con las buenas características de robustez.

Al ambiente de prueba no se le daba la importancia necesaria, no contaba con un dominio para aplicar políticas de seguridad. Era muy improvisado. Más allá que los recursos eran escasos, viejos y casi obsoletos, había también desaprovechamiento de recursos por no estar dentro de un cluster.

Con esta nueva estructura, se armó un cluster exclusivo de test, junto con políticas propias de seguridad, con red independiente, dominio independiente, y con la capacidad suficiente para recrear réplicas casi idénticas a los sistemas de producción. Todo totalmente aislado y también visualizado desde el mismo vCenter. Al contar con dominio, permitía aplicar políticas muy similares a las de producción. Con este nuevo ambiente más robusto y con una emulación más precisa a la de producción, disminuía las tareas de rollback, aumentando considerablemente las implementaciones, tanto en nuevos sistemas como en modificaciones de los ya existentes.

6.3.3 Herramienta para clonar VMs a diferentes clusters.

La herramienta de clonado permite realizar una copia exacta de una VM, que puede ser destinado para un mismo cluster o para otro distinto, pero administrado por el mismo vCenter. Facilita las tareas de nuevas implementaciones, actualizaciones de sistemas y actualizaciones del SO y software de base.

El clonado realiza una copia exacta de toda una VM. Al momento de seleccionar el destino se colocaba en el cluster que se desee, por ejemplo el de test. Se le cambia la IP por una del rango de test, se coloca en el demonio de Test y se reconfiguran los sitios y permisos teniendo en cuenta la seguridad en ese ambiente. Y en cuestión de poco tiempo, ya se tiene un server con todas las características necesarias en un ambiente totalmente diferente y listo para realizar los cambios y pruebas requeridas sin intervenir con la disponibilidad del server productivo.

Otro caso muy útil, por ejemplo, se da cuando el server de producción tiene varias actualizaciones y modificaciones aplicadas y que en test nunca las replicaron. Por lo que el server para realizar testeos ya no cumple con las características necesarias para que las pruebas sean un buen indicio de lo que podría pasar en producción. En estos casos, y para ahorrar tiempo y trabajo, lo más práctico es eliminar la VM de test, y mediante la herramienta de clonado, se crea una nueva copia exacta del server de producción, dejándola disponible en test, lista para trabajar.

Otro ejemplo es cuando se debe implementar nuevos sistemas en servers dedicados. En estos casos se prepara la VM con todos los requisitos necesarios en el ambiente de test, se instala el sistema nuevo, se realizan las pruebas y correcciones necesarias, y cuando se considere que ya está listo, su paso a producción es muy sencillo. Se clona esa VM a producción, se reconfigura para dejarla operativa en el nuevo ambiente y listo, en minutos ya se encuentra en línea.

6.3.4 Snapshots –agilizar nuevas implementaciones.

Un Snapshots es una imagen del Server, manteniendo todo el estado de esa VM, conservando el estado de memoria, discos, etc. Es una herramienta muy usada cuando hay nuevas implementaciones o actualizaciones de SO o de software base, tanto en test como en producción

Un caso de uso muy común es, si la nueva implementación implica cambios donde no se sabe las secuelas que podría provocar, como por ejemplo que no levanten o generen un error indeseable que no era tenido en cuenta. Antes de hacer esas modificaciones, se le puede aplicar un snapshots a ese server. Esto permitía que el rollback sea más seguro, porque se hace a nivel de VM, y muy rápido

Otro caso muy común es cuando, si bien las modificaciones no implicaban grandes cambios, pero el sistema en cuestión interactúa con varios sistemas en distintos servers, con muchos parámetros de seguridad. Entonces las pruebas que se hacían en test, por más que funcionaran, no aseguraban que pasarlas a producción funcionaran al 100%. Por lo que era muy común realizar un snapshots para que el rollback, sea más inmediato.

6.3.5 Mayor disponibilidad de recursos

Esta facilidad de hacer snapshots y poder mantenerlo por varios días, mientras se realicen todos los cambios correspondientes a una implementación, como también la de clonar VMs y mantenerla apagada por un tiempo es más factible gracias a la agrupación de host en clusters. La ventaja es notoria en cuanto a disponer de los recursos de varios hosts agrupados en un cluster, donde todos los recursos se ven como un todo. En cambio, contar con los mismos recursos, pero independiente en cada host, si bien es la misma cantidad, pero al estar fragmentado es mucho más acotado.

Con un ejemplo se puede entender mejor. Si hay una VM activa muy grande, que tiene dos discos de 200 y 400 GB C/U, con un 75% ocupado, y además tiene una configuración de 16 CPU y 24 GB de RAM. Si se tiene en cuenta que un host tiene varias VM virtuales, poder replicar este server ahí mismo es muy probable que no sea posible. Y en caso de ser posible, puede dejar al host muy saturado provocando mala performance en el resto de las VMs.

Esta misma situación, pero en un cluster con varios hosts, como hace una redistribución automática de recursos y además cuenta con Datastores compartidos, ubica el clonado en el host más conveniente, de acuerdo a la disponibilidad de recursos, sin comprometer la funcionalidad del resto de los hosts y de las VMs.

6.3.6 Facilidad para actualizar versiones y parchado de SO

En estructuras de Data Center con cientos de servidores y mucha información a procesar, es importante contar con soporte oficial. Puntualmente con los servers con Sistemas Operativos Microsoft.

Para mantener el soporte oficial los SO deben tener versiones recientes. Por lo que es necesario ir actualizando los sistemas operativos, antes de caducar el soporte oficial. Además, los beneficios no son solo por soporte oficial. Los servicios de las entidades están en constante cambio, y es importante usar tecnología más reciente para mantener la mayor compatibilidad posible, como también actualizarse ante nuevas vulnerabilidades de seguridad. Es decir, mantener actualizado los Sistemas Operativos es considerado como parte de las buenas prácticas.

Este proceso lleva mucha planificación. Porque significaba un retrabajo constante y la interrupción de los servicios. La planificación tiene mucha gradualidad, los parchados y actualizaciones implican tiempo de indisponibilidad de servicios. Las herramientas como snapshots y la clonación, permiten que esas interrupciones disminuyan considerablemente. Y nuevamente cabe resaltar que sin una estructura de clúster administrada por vCenter vSphere, las migraciones masivas de actualización, no podría llevarse a cabo, o quizás sí, pero con grandes interrupciones. Lo que influye directamente en la calidad del servicio de la organización.

6.3.7 Estructura física que acompañe los cambios del negocio.

Las empresas que se ven enfrentadas a una feroz competencia y con Centros de Datos con alta disponibilidad, están en constantes modificaciones y crecimiento, Cada vez se ofrecen más servicios, muy diversos, con disponibilidad constante, con importantes campañas para atraer a nuevos clientes. Las billeteras virtuales, obras sociales, servicios de movilidad, etc. son algunos de los ejemplos de los rubros que adoptan estas características. Esto trae aparejado un aumento significativo y constante, muy difícil de visionar y que no cesa. La cantidad de servidores cada vez son más, y es inevitable que también crezca la estructura física para aumentar la capacidad de procesamiento y almacenamiento.

Hoy en día es difícil imaginar que un Data Center sin una administración centralizada y sin las herramientas como vsphere, sea suficiente para acompañar las prestaciones necesarias de cualquier organización que opere con las cambiantes reglas del mercado actual.

En este nuevo Data Center Centralizado, aumentar la capacidad de procesamiento es mucho más simple, sin necesidad de grandes planificaciones. Solo con agregar uno o dos hosts más a un cluster, y agregar discos a los array de Datastore, ya se aumenta la capacidad para soportar un buen crecimiento, sin interferir en la disponibilidad del funcionamiento integral del sistema. Obviamente no estamos considerando el costo de los equipos y de las licencias, solo nos referimos a la parte técnica.

Cuando se agregan hosts a un cluster que cuenta con DRS y vMotion, automáticamente los servidores van migrando a los nuevos hosts disponibles para dejar balanceada la carga de los recursos, y todo en caliente y con un mínimo de interrupción, casi imperceptible, sobre los servicios.

Lo único que hay que tener en cuenta es que el host a agregar sea del mismo modelo y marca que el resto de los que tiene el cluster, y además debe tener la misma versión de ESXi. Configurándolo en la misma Red que el resto, no presente inconvenientes.

No es del todo necesario que los hosts a agregar tengan el mismo modelo y marca, con que tengan hardware compatible, ya es suficiente. Pero como una buena práctica, lo más recomendable es que sean exactamente iguales.

6.3.8 Facilidad para evolucionar la infraestructura de hardware.

Mantener una buena performance, también implica mejorar la estructura física. Es así que implementar un nuevo cluster con host más modernos, más potentes, con mayores prestaciones, como así también con Datastore más ágiles, potentes y con mayor capacidad de almacenamiento, migrarlo no es para nada complicado con respecto a la original.

Se define las necesidades de hardware, teniendo en cuenta la tasa de crecimiento a nivel estructura. Se prepara toda la nueva estructura paralelamente a la actual. Colocación en los racks físicos correspondientes, instalación del ESXI, actualización y colocación de las licencias correspondientes, y finalmente el armado del cluster nuevo dentro del mismo vCenter donde está el actual cluster productivo. Aplicando todas las configuraciones correspondientes

Luego queda el paso más complejo, migrar las VMs de un cluster al nuevo. Esto es mucho más sencillo, porque con la herramienta vMotion, se puede hacer en caliente. Pero para no saturar la red, y al contar con herramientas más potentes, es posible adoptar una planificación más holgada, evitando entorpecer la migración y la performance del sistema. Permitted programar estos movimientos en horarios de menor demanda de los sistemas, priorizando pasar primero los que tienen menor demanda y de menor tamaño, dejando para el último a los de mayor demanda y tamaño. Estas migraciones se pueden programar con PowerCLI, facilitando la menor intervención de los Administradores y que se ejecuten en horarios con muy poca demanda de servicios. Migrar a una nueva estructura se torna 100% inadvertida por las demás áreas y principalmente por los clientes. Y se puede llevar a cabo en solo meses. Y también es importante tener presente la seguridad y el casi nulo estrés que tuvieron en esta ocasión los responsables de la migración. Un tema no menor

6.3.9 Plantillas para agilizar la creación de nuevos servers

La generación de plantillas (templates) en VMware vCenter es una funcionalidad clave para estandarizar e implementar rápidamente máquinas virtuales (VM)

Una plantilla VM es una imagen de copia maestra de una máquina virtual que incluye discos VM, dispositivos virtuales y ajustes. Puede utilizarse varias veces para clonar máquinas virtuales. No es posible encender y editar la plantilla una vez creada. Esto es por diseño, para que nadie pueda editar accidentalmente la máquina virtual que se utiliza como plantilla. Después de clonar la VM desde una plantilla, los clones VM no están vinculados a una plantilla VM y son independientes.

Las plantillas de VM son útiles para desplegar un gran número de VM similares, ya que preservan la consistencia de la VM. Por ejemplo, suponiendo ante una nueva implementación, se necesita realizar varias pruebas en máquinas virtuales con una nueva versión de uno de sus sistemas. El administrador de sistemas de la empresa crea una plantilla de máquina virtual con todos los requerimientos solicitados y clona una máquina virtual idéntica a partir de esa plantilla para cada trabajador que necesite una.

La gran ventaja del uso de plantillas es q permite clonar entornos preconfigurados (OS, aplicaciones, parches) en minutos, ahorrando tiempo, reduciendo errores manuales y garantizando la consistencia en la infraestructura. Es una herramienta que permite mayor escalabilidad de un Data Center.

6.3.10 Actividades para mantener la performance del Data Center.

Con la herramienta vReleaze y RVTools se pueden obtener información que permite tomar medidas proactivas para mantener la buena funcionalidad del Cluster

- **Borrado de Snapshots antiguos.** Un snapshot no es una copia completa inicial de los datos de una VM; es una imagen del estado de un disco en un momento exacto. Al inicio el tamaño del snapshot es casi cero porque solo contiene metadatos. Pero con el tiempo, cuando modificas o eliminas un archivo en el disco original, el sistema debe preservar el bloque de datos antiguo para que el snapshot siga siendo válido. Ese bloque se guarda en el archivo del snapshot, haciendo que este crezca. El tamaño del snapshot no depende de cuántas horas pasen, sino de la actividad de escritura en los discos. Si se instala programas, borran archivos grandes o desfragmenta el disco, el snapshot crecerá rápidamente ya que registra cada uno de esos cambios. Cuanto más tiempo mantengas un snapshot activo, más cambios acumulará respecto al estado original, pudiendo llegar a ocupar el mismo tamaño que el disco base. Un snapshot muy grande o mantenido por mucho tiempo puede degradar el rendimiento de la máquina virtual o el servidor. Y si no se monitorean, pueden llenar el almacenamiento físico (datastore), provocando la caída de los sistemas. Muchas veces los snapshots se mantienen más de la cuenta, por pedido de los desarrolladores que realizaron nuevas implementaciones. Una de las medidas que se pueden tomar es generar listados de VMs con snapshots mayor a cierta cantidad de días para tener en cuenta eliminarlos. Antes de eliminarlas, siempre se consultan con los implementadores.
- **Alertas de VMs apagadas después de cierto tiempo.** Muchas veces se clonan máquinas temporales y solicitan mantenerla algún tiempo, y al pasar un tiempo queda sin borrarse. O por ejemplo servers que ya no se usan más, también se decomisan
- **Modificar los recursos de los servidores,** ya sea aumentándolos o disminuyéndolos. Nos referimos al número de CPU y Memoria de acuerdo al promedio de uso. Info que se obtiene con vReleaze. Las nuevas versiones permiten aumentar la CPU y la Memoria en caliente. Es muy ventajoso para poder salir de imprevistos que suceden con demandas picos. En cambio, para disminuir los recursos, es necesario que la VM esté apagada. Para estos casos se planifica hacerlo fuera del horario de mayor demanda y cuando los servicios del server en cuestión tengan la menor actividad. Lo bueno es que la interrupción, en la mayoría de los casos, no supera el minuto.
- Otro alerta que ayuda mucho es **controlar el almacenamiento de los servidores.** Con RV Tools puede obtener el porcentaje de ocupación de cada uno de los discos. Eligiendo un umbral que sea inferior al 75% ocupado, para evitar no saturar los servidores. En caso de haber alertas, se consultan con diferentes sectores para depurar info o bases para liberar espacio (logs muy grandes, archivos temporales que no se eliminan, etc). Y en caso de no encontrar nada para poder liberar, se extiende el tamaño del disco en caliente, sin interrumpir la actividad del servidor.
- **Aplicar planificaciones para modificar los recursos de una VM asignando recursos on-demand:** Hay servidores que tienen una sobrecarga muy elevada, pero es temporal. Quizás sea una vez al mes o con menor frecuencia. Asignarles muchos recursos de CPU y memoria para que funcione de manera correcta al momento de tener esta gran demanda, y que durante el resto del tiempo ocupa menos del 10%, es un desperdicio de recursos que condiciona a la estructura. En estos casos se los puede asignar un número de recursos

standard, y al momento de correr estos grandes procesos, se los puede aumentar de acuerdo a la necesidad. Y una vez finalizado, se deja como lo tenía anteriormente. Esta buena práctica beneficia a que el DRS funcione mejor, cuando el server no ocupa los recursos necesarios

- RVTools también se usa como una **herramienta de auditoría y visibilidad**, permitiendo anticipar problemas (rendimiento, espacio, seguridad) antes de que impacten a los usuarios, en lugar de solo reaccionar a ellos, mediante reportes detallados y exportables. Algunas medidas proactivas a partir de RVTools:
 - Gestión de Almacenamiento: Reporta discos virtuales dinámicos grandes que podrían beneficiarse de ser convertidos a tamaño fijo para mejor rendimiento. Además identifica los discos virtuales que crecen excesivamente, previniendo problemas de capacidad y poder analizar el inconveniente. Y se puede tener presente el estado de los Datastore.
 - Mantenimiento del Entorno: Obtener un inventario completo de VMs, hosts, redes y almacenamiento para detectar anomalías.
Identificar plantillas antiguas o no utilizadas que necesitan ser limpiadas.
Verificar el estado de servicios críticos de vSphere (HA/DRS) para asegurar la alta disponibilidad.
 - Seguridad y Cumplimiento: Identificar versiones antiguas de VMware Tools o de firmware/hardware que puedan representar vulnerabilidades.
 - Planificación y Reportes: Usar la función de fusión de XLSX para consolidar datos de múltiples vCenters y obtener una vista unificada. Utilizar los datos para planificar futuras expansiones o migraciones, entendiendo el consumo actual de recursos.

6.3.11 Optimizar el almacenamiento. Distintos tipos de Aprovisionamiento.

Hay dos grandes tipos de aprovisionamiento para configurar los discos de las VMs. Aprovisionamiento fino y grueso.

El aprovisionamiento grueso (**thick**) reserva todo el espacio del disco virtual al crearlo, garantizando rendimiento predecible, pero consumiendo más espacio físico inicialmente. Y el aprovisionamiento fino (**thin**) asigna espacio solo cuando los datos se escriben, optimizando el almacenamiento físico, pero requiriendo monitoreo para evitar llenarse.

Thin Provisioning empieza con un archivo VMDK casi vacío. El espacio físico se asigna solo a medida que la VM escribe datos en él, expandiéndose dinámicamente. La gran ventaja es que ahorra espacio en el almacenamiento, permitiendo sobreaprovisionar (asignar más espacio del disponible). Pero si el almacenamiento físico se llena, la VM puede fallar; requiere monitoreo constante.

Lo bueno es que con el tiempo y de acuerdo a las necesidades del server, se puede cambiar el tipo de aprovisionamiento de manera sencilla. Conviene apagar el server, y realizar una migración de almacenamiento, eligiendo la opción de aprovisionamiento diferente a la original. Esto, de acuerdo al tamaño del disco, no toma más de algunos minutos. Por lo que la falta de disponibilidad no es tan alta. Y en caso de necesitar una alta disponibilidad, se analiza un horario conveniente para realizarlo.

6.3.12 Herramientas de Backup y Recovery

Estas herramientas de backup y recuperación para vCenter ofrecen grandes ventajas como la protección integral de VMs, recuperación rápida y continuidad del negocio. Aunque presentan desventajas que son muy importantes al momento de pensar en implementarlas, como alto

consumo de recursos, costos elevados, complejidad en la configuración inicial y dependencia de la infraestructura de hardware subyacente, requiriendo soluciones dedicadas para la protección eficiente de cargas de trabajo virtualizadas.

Es necesaria una solución de backup dedicada (ya sea nativa o de terceros) para proteger las VMs de forma eficaz. Generalmente se usan herramientas de terceros como Veeam, Vinchin o Nakivo que se integran con vCenter ofreciendo más funciones y a menudo sin agentes.

Existen varias situaciones que pueden provocar la inaccesibilidad de una VM.

- Espacio insuficiente en el datastore.
- Desconexión o pérdida del almacenamiento
- Errores de consolidación. Sucede cuando falla la integración de un snapshot, ya sea por su gran tamaño o por falta de espacio en sus discos.
- Error en la actualización de un parchado del SO, generalmente porque la cantidad de parches es grande.
- Errores humanos, como la eliminación accidental del inventario o del datastore.

Es en estos casos donde las herramientas de backup y recuperación dan un respiro importante a la organización. Se puede restaurar la VM afectada rápidamente, minimizando el tiempo de inactividad, asegura la supervivencia de datos críticos, ahorrando costos y tiempo, y asegurando la disponibilidad de los servicios.

También se puede realizar una recuperación Granular, es decir restaurar archivos individuales, no solo la VM completa, facilitando la recuperación de datos específicos.

A diferencia de las instantáneas (snapshots) que son temporales, consumen recursos y deben usarse con precaución. No se las puede considerar backups. En cambio, los backups de VMs se almacenan en Datastores externos e independientes.

6.3.13 Fácil visualización de alertas de hardware

vCenter facilita la visualización de alertas de hardware centralizando la información en un único panel, permitiendo ver el estado de hosts ESXi y VMs, y configurar notificaciones (Dashboards, Eventos, Notificaciones). Las alertas pueden referirse a problemas de discos, memoria, red y sensores de temperatura y energía, Pueden ser advertencias, errores o críticos. Si bien esto es de gran ayuda para tomar medidas, pero para una mayor profundidad de análisis, se recomiendan herramientas como OpManager o PRTG.

Tipos de visualizaciones nativas de vCenter

Centro de Alertas (Alarm & Events): En la interfaz de vSphere, el panel Monitor y Eventos muestra alertas en tiempo real del hardware y las VMs, con opciones para filtrar por criticidad.

Monitorización de Hosts: Puedes seleccionar un host ESXi individual y ver su estado de hardware, incluyendo sensores, discos, y otros componentes físicos a través de la interfaz. El BMC (controlador de administración de placa base) es muy usado para ver más detalladamente el error de hardware.

Dashboards Personalizados: Crea dashboards que consoliden la información de hosts, clústeres y VMs en un solo lugar para una visión rápida del estado general.

Una práctica muy común es configurar umbrales personalizados para métricas de rendimiento y hardware para recibir alertas proactivas antes de que ocurran fallos mayores. Esto colabora a ocuparse de solucionar los inconvenientes con la mayor antelación posible. Permitiendo planificar e interrumpir lo menos posible la disponibilidad de los servicios.

Un ejemplo, cuando un host visualiza alta carga de cpu y/o memoria. En esos casos una solución rápida es pasar VMs por vMotion a otros host más holgados en consumo de recursos y sin interrupción del funcionamiento. Y evita el colapso de cualquier host.

Algunas alertas visualizan inconvenientes de hardware, que requieren el reemplazo de una pieza, ya sea cable de conexión de red o energía, fuentes power, memoria, discos, etc. Algunas se pueden reemplazar en caliente y otras necesitan del apagado del host. En cualquier caso es recomendable migrar todas las VMs de host al resto de los hosts, y colocarlo en modo mantenimiento. Así se puede disponer del host para trabajarlo tranquilamente. Esto es posible gracias a que las alertas permiten planificar soluciones sin la presión de la inmediatez.

6.4 Características indispensables de un Data Center

Si nos referimos a grandes organizaciones cuyos servicios funcionan 24x7, los 365 días del año, sumado a que operan en un mercado con constantes cambios de reglas, es esencial contar con una estructura de sistemas que acompañe este escenario. Por eso las características de robustez, alta disponibilidad y buena escalabilidad, son indispensables en un Data Center.

6.4.1 Buena escalabilidad.

Como se analizó en capítulos anteriores, en un Data Center sin administración centralizada y sin clusters, la escalabilidad es muy complicada, casi escasa. Aumentar servicios y recursos implica no solo una gran planificación, sino una gran interrupción de los servicios. Afectando directamente a la calidad e imagen de la organización.

Por ejemplo, en una Data Center con poca virtualización, con estructura no integrada y procesando de manera aislada, es muy común encontrarse con viejos hosts que contienen varias VMs, pero una o dos de ellas, con el paso del tiempo, se convertían en grandes servidores, con grandes almacenamientos, demanda constante y alto grado de procesamiento. Transformándose en VMs monstruosas y a la vez indispensables para el negocio. En situaciones así, la primera solución que se le viene en mente a cualquier Administrador, es aumentar los recursos. Lo más común, adquirir nuevos hosts que ofrezcan mayor procesamientos y almacenamiento. El problema es que este nuevo hardware no brindaba una solución de fondo. Esas grandes VMs son tan complicadas migrarlas, que se optaba por migrar al nuevo hardware los servers de menor tamaño, los que no tenían tantos inconvenientes con la interrupción de su funcionamiento. La tendencia es que los servers de gran tamaño, con una gran importancia en su disponibilidad, continuaran funcionando sobre estructuras obsoletas, con el riesgo que esto conlleva. Se evidencia una escalabilidad sumamente limitada y sin grandes mejoras.

En cambio, si nuestro Data Center funciona sobre distintos clusters, administrados por vSphere vCenter, la capacidad de procesamiento y almacenamientos se ve como un todo. Literalmente está disponible para todos los servers por igual. Llegado el momento de tener que aumentar los recursos físicos, con el solo hecho de agregar más hosts al cluster y/o agregar nuevos datastores o más discos a los datastores existentes, directamente es brindarle más recursos a cualquier server virtual que funcione sobre ese cluster. Con una interrupción mínima de sus servicios, y en muchos casos, con una interrupción nula. La escalabilidad es prácticamente un comportamiento natural en este tipo de infraestructuras.

Además, el clonado de VMs, trabajar con plantillas, los snapshots, tener un buen ambiente de test totalmente aislado y de fácil administración, permite que las nuevas implementaciones sean mucho más ágiles, al igual que la actualización del software base de las VMs. Esto también le da características de escalabilidad al Data Center.

Otro punto importante, la facilidad con la que vCenter puede agregar un nuevo cluster integrado por hosts con tecnología más moderna, potente y con mayor capacidad. Hay varias herramientas para migrar al nuevo cluster, mayor cantidad de VMs en menor tiempo. Permite actualizar la tecnología de la infraestructura del Data Center, sin faraónicas planificaciones y con poca intervención de terceros. Situación muy distinta a cuando se migra de un Data Center tradicional no centralizado, a uno con clusters y administración centralizada

6.4.2 Alta Disponibilidad (HA)

En informática, “Alta Disponibilidad” hace referencia a que los servicios se mantengan siempre activos. Ante cualquier eventualidad que tengan la menor interrupción, y dentro de lo posible, que esa interrupción sea nula. La alta disponibilidad es uno de los principales beneficios obtenidos en este nuevo paradigma de Data Center. Esta característica es lo más importante por cualquier empresa que desea ofrecer calidad en sus servicios. Tanto vMotion como DRS, son las principales funcionalidades que permite la HA. Además, hay herramientas que permiten una mayor HA para aquellos servers que lo requieran, por ejemplo FT (Fault Tolerance), con cero tiempo de inactividad.

Como se mencionó en el punto anterior sobre la escalabilidad, hay varias herramientas y actividades que también dan característica de Alta Disponibilidad a un Data Center. La facilidad para migrar a nuevo hardware más potentes, contar con un robusto ambiente de prueba, clonado VMs, usar plantillas para agilizar la creación de nuevos servers, los snapshots temporales, poder planificar la actualización del software base de las VMs con mayor eficiencia, planificar cambios e implementaciones con la menor inactividad posible, contar con monitoreo que permite tomar medidas proactivas, etc., colaboran a que la interrupción de la funcionalidad de los servicios se evite lo más posible, mientras se tejen diferentes cambios por debajo de la funcionalidad.

Y una característica importante para que un Data Center tenga una buena HA, es contar con herramientas de Backup Recovery y Réplica. Ante grandes desastres catastróficos, permite que el Data Center se recupere rápidamente.

6.4.3 Facilidad para implementar actividades proactivas

Para que un Data Center mantenga las características de Alta Disponibilidad y Buena Escalabilidad, es necesario que haya un buen mantenimiento del sistema. Se deben realizar tareas para evitar que se produzcan errores que pueden significar un alto costo a la organización, es decir tener una actitud proactiva.

vSphere vCenter cuenta con monitoreo y alertas fácilmente visibles. Es una herramienta que además de mostrar errores de hardware, se puede configurar para generar alertas por el uso de recursos que superan un umbral especificado. Permitiendo ocuparse del incidente de manera inmediata. En la interfaz de vCenter, se pueden visualizar fácilmente las alertas, además de distinguir si es nivel cluster, hosts, VM, red, datastore etc. Por otro lado vRealize logs Insight facilita detectar la anomalía con mayor precisión

La herramienta RVTools es muy usada para detectar situaciones que se pueden mejorar. Por ejemplo; liberar espacio en Datastore; detectar si una VM necesita modificar sus recursos;

detectar crecimiento inusual en VMs, Datastores o Hosts; versiones desfasadas de hosts, vmttools, SO; etc. Estos reportes generan tareas que permiten un buen mantenimiento del DataStore.

6.4.3.1 vRealize Operations

En un entorno vCenter, el uso de vRealize Operations – vROps, permite pasar de una administración reactiva a una proactiva y predictiva. Algunas medidas proactivas que se pueden tomar usando esta herramienta.

- **Planificar ampliaciones de hardware para evitar saturar los recursos.**
Una tarea importante que se puede obtener a partir de vRealize Operations es Monitoreo proactivo de capacidad. A partir de analizar CPU, memoria, almacenamiento y red en hosts, clústeres y VMs, se pueden detectar tendencias de crecimiento, basado en estadísticas históricas. Puede predecir con gran exactitud los días, semanas o meses en la que se agotarán los recursos. Esta información también permite redistribuir VMs entre clústeres para evitar cuellos de botella.
- **Optimización continua de recursos.**
Analiza el uso de los recursos a nivel de VMs. Se obtienen promedios que detecta sobredimensiones de vCPU o RAM. O VMs infrautilizadas o inactivas. Y también VMs con configuración ineficiente. A partir de estos análisis, se pueden realizar recomendaciones, ya sea para reducir recursos o aumentarlos, y así evitar saturación del server. Es muy común que haya sobredimensión de recursos, lo que se puede liberar recursos que permiten un funcionamiento de hardware más eficiente.
- **Alertas preventivas de incidentes**
A diferencia de vCenter, que alerta por eventos simples, vROps asocia métricas, síntomas y causas raíz. Esto detecta degradaciones de manera progresiva, generando alertas para tomar medidas correctivas de manera anticipada. Por ejemplo, un aumento progresivo de latencia de disco, alerta antes de que la VM quede inoperativa.

CONCLUSIONES

Este trabajo permitió analizar todo el proceso de migración de un Data Center tradicional, compuesto por servidores heterogéneos administrados individualmente, a un entorno completamente virtualizado y gestionado de forma centralizada mediante VMware vSphere y VMware vCenter Server, obteniendo una visión global de toda la estructura.

Se comenzó describiendo la arquitectura del modelo tradicional, con sus grandes limitaciones como la alta dependencia del hardware subyacente, desaprovechamiento de los recursos disponibles, dificultades en la administración, ausencia de automatización y escalabilidad muy baja, con frecuentes fallas que aumentaban la interrupción de los servicios. Inconvenientes que justifican la necesidad de un cambio radical en la gestión de la infraestructura.

La virtualización usando hosts con VMware ESXi y almacenamiento compartido, todo interconectado con redes de alta velocidad, permite abstraer los recursos físicos para administrarlos de manera unificada. Además, la incorporación de clústeres, posibilita la distribución dinámica de cargas de trabajo y la alta disponibilidad, reduciendo significativamente las fallas de hardware, aumentando significativamente la performance del Data Center.

Las funciones más destacables como vMotion, DRS y High Availability (HA) demostró el impacto directo en la continuidad del negocio, al minimizar el downtime y permitir tareas de mantenimiento con interrupciones mínimas de sus servicios. La comparación de los procesos antes y después de la migración evidenció mejoras sustanciales en actualización, ampliación de recursos, recuperación ante fallos y monitoreo centralizado. Esta estructura permite agregar más herramientas, dejando muy atrás una gestión reactiva, pasando a ser proactiva.

VMware vSphere vCenter es considerada una de las mejores herramientas para gestionar Data Center con gran volumen de servicios que requieren alta disponibilidad, pero su gran desventaja es su elevado costo. Implementar este tipo de Data Center representa grandes inversiones en hardware y software. Tener en cuenta que un factor importante para que cualquier organización ofrezca calidad, en gran medida está dado por el estado de su Data Center.

Este nuevo paradigma de gestión no solo optimiza el uso de los recursos tecnológicos, sino que también mejora la escalabilidad, la flexibilidad operativa y la capacidad de crecimiento futuro. Esto determina que la migración hacia un Data Center virtualizado y centralizado no solo representa una actualización tecnológica, sino una transformación estratégica orientada a la eficiencia, resiliencia y alineación a las necesidades actuales y futuras de la organización.

Quien presenta este informe formó parte de un equipo que en un lustro materializó este “cambio de paradigma” habiendo visualizado y comprobado las desventajas del modelo anterior y disfrutar en la actualidad, de las mejoras y ventajas de la virtualización.

Debido a la confidencialidad establecida por la organización respecto a la tecnología utilizada, arquitectura, datos y configuraciones adoptadas, no es posible disponer de la información necesaria que permita reflejar cualitativa y cuantitativamente las mejoras alcanzadas con la incorporación de las nuevas aplicaciones.

Por ello como corolario de las presentes conclusiones y dada la imposibilidad de contar con datos reales de la organización donde se llevó adelante la aplicación, me permito presentar una solicitud elevada a la IA ChatGPT que atento a la problemática tratada a lo largo del trabajo,

realice el **Planteamiento de una instancia de virtualización de un sistema en el marco de una organización dada** mediante la escritura del siguiente prompt “*En la migración de un Data Center tradicional con servidores físicos heterogéneos administrados individualmente a una Data Center Virtual administrado de manera central con VMware vCenter Server y con clusters. Cuáles son los parámetros medibles en porcentaje que demuestren las mejoras entre la estructura tradicional y la actual?*”; expone una tabla comparativa “antes y después” que se puede utilizar para ilustrar las mejoras de una migración.

Parámetro	Data Center Tradicional	Data Center Virtualizado	Mejora aproximada
Utilización promedio de CPU	15–25 %	60–80 %	+200 % a +300 % de eficiencia
Utilización de memoria RAM	20–30 %	65–85 %	+180 % a +250 %
Cantidad de servidores físicos	40	6 hosts	–85 % de hardware
Disponibilidad del servicio (Uptime)	97–98 %	99.9 %	Reducción >90 % del downtime
Tiempo de aprovisionamiento de servidores	2–5 días	10–20 minutos	–99 % del tiempo
Tiempo de recuperación ante fallos (MTTR)	2–4 horas	5–10 minutos	–90 % a –95 %
Balanceo de carga entre servidores	Manual o inexistente	Automático mediante cluster	+80 % de eficiencia
Tiempo dedicado a administración	20 h/semana	5 h/semana	–75 %
Consumo energético del Data Center	12 kW	4 kW	–66 %
Uso del almacenamiento	40–50 %	70–85 %	+40 % a +60 %

Si bien esta comparación demuestra que la virtualización con gestión centralizada permite obtener una mayor eficiencia en el uso del hardware, una mayor disponibilidad de los servicios, una reducción significativa de los tiempos operativos y una disminución considerable del equipamiento físico y del consumo energético, estos indicadores no alcanzan a reflejar plenamente el profundo cambio que implica la adopción de estas tecnologías.

No solo se optimiza la eficiencia de los servicios, sino que también incorpora un nuevo paradigma de gestión, más organizado, flexible y completamente proactivo.

BIBLIOGRAFIA

1. Red Hat Enterprise Linux. ¿Qué es la virtualización?
<https://www.redhat.com/es/topics/virtualization>. 2025.
2. Red Hat Enterprise Linux. ¿Qué es un hipervisor?
<https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor>. 2023.
3. IBM Corp. ¿Qué es VMware?. <https://www.ibm.com/es-es/think/topics/vmware>. 2025
4. IBM Corp. ¿Qué es VMware?. <https://www.ibm.com/es-es/think/topics/vmware>. 2025
5. IONOS Inc. ¿Qué es ESXi y qué ventajas ofrece este hipervisor?.
<https://www.ionos.com/es-us/digitalguide/servidores/know-how/esxi/>. 2025
6. IONOS Inc. ¿Qué es ESXi y qué ventajas ofrece este hipervisor?.
<https://www.ionos.com/es-us/digitalguide/servidores/know-how/esxi/>. 2025
7. Broadcom Inc. <https://techdocs.broadcom.com/es/es/vmware-cis/vsphere/vsphere/7-0/vcenter-and-host-management-7-0/vsphere-concepts-and-features-host-management.html>. 2025
8. Robert Sheldon, Brien Posey, TechTarget Inc. What is VMware vSphere?
<https://www.techtarget.com/searchvmware/definition/VMware-vSphere>. 2024
9. Federico Cinalli, OpenWebinars S.L. Almacenamiento en vSphere.
<https://openwebinars.net/blog/almacenamiento-en-vsphere/>. 2019
10. Jeremías Palazzesi. Configuración VMWare VCenter.
<https://www.nerdadas.com/blog/configuracion-de-red-y-vlans-en-vmware-vcenter/>. 2022
11. Broadcom Inc. Introducción a redes de vSphere.
<https://techdocs.broadcom.com/es/es/vmware-cis/vsphere/vsphere/9-0/vsphere-networking/introduction-to-vsphere-networking.html>. 2025
12. Broadcom Inc. Configuración de VLAN. <https://techdocs.broadcom.com/es/es/vmware-cis/vsphere/vsphere/9-0/vsphere-networking/isolate-network-traffic-by-using-vlans/vlan-configuration.html>. 2025
13. Nakivo Inc. <https://www.nakivo.com/es/blog/vmware-vsphere-7-installation-setup/>. 2024
14. Broadcom Inc. Introducción a la instalación y configuración de vSphere.
<https://techdocs.broadcom.com/es/es/vmware-cis/vsphere/vsphere/7-0/vcenter-server-installation-and-setup-7-0/introduction-to-vsphere-installation-and-setup.html>. 2025
15. Broadcom Inc. Descripción de vCenter Server Appliance.
<https://techdocs.broadcom.com/es/es/vmware-cis/vsphere/vsphere/7-0/vcenter-server-installation-and-setup-7-0/introduction-to-vsphere-installation-and-setup/overview-of-the-vcsa.html>. 2025
16. Broadcom Inc. Implementar vCenter Server Appliance.
<https://techdocs.broadcom.com/es/es/vmware-cis/vsphere/vsphere/7-0/vcenter-server-installation-and-setup-7-0/deploying-the-vcenter-server-appliance.html>. 2025

17. Nakivo Inc. Guía de instalación de VMware vCenter y prácticas recomendadas. <https://www.nakivo.com/es/blog/vmware-vcenter-deployment/>. 2024
18. Soha Fouad, VMware by Broadcom Inc. VMware vSphere Cluster Services Explained. <https://blogs.vmware.com/cloud-foundation/2022/06/09/vmware-vsphere-cluster-services-explained/>. 2022
19. Broadcom Inc. Cómo crear un clúster de vSphere con vSphere Client <https://techdocs.broadcom.com/es/es/vmware-cis/vsphere/vsphere/8-0/create-a-cluster.html>. 2025
20. Nakivo Inc. Configurando un clúster de VMware ESX. <https://www.nakivo.com/es/blog/configuring-vmware-esxi-cluster/>. 2024
21. Nick Zhao. Chengdu Vinchin Technology Co., Ltd. What Is vMotion and How to Migrate VM in vCenter Step by Step? <https://www.vinchin.com/vm-migration/vmware-vmotion.html>. 2024
22. Nakivo Inc. Comparación y explicación de VMware vSphere HA y DRS. <https://www.nakivo.com/es/blog/vmware-vsphere-ha-and-drs-compared-and-explained/>. 2024
23. Nakivo Inc. Cómo Configurar HA en VMware vSphere. <https://www.nakivo.com/es/blog/vmware-cluster-ha-configuration/>. 2024
24. Broadcom Inc. Funcionamiento de Fault Tolerance. <https://techdocs.broadcom.com/es/es/vmware-cis/vsphere/vsphere/8-0/vsphere-availability/providing-fault-tolerance-for-virtual-machines/how-fault-tolerance-works.html>. 2025
25. Nakivo Inc. Cómo instalar VMware Tools en Linux, Windows, MacOS, FreeBSD y Solaris. <https://www.nakivo.com/es/blog/how-to-install-vmware-tools-on-guest-os-overview/>. 2025
26. Arsys de IONOS Group. Manuel León. ¿Qué son las VMware Tools? <https://www.arsys.es/blog/que-son-vmware-tools>. 2025
27. Nakivo Inc. Cómo instalar VMware PowerCLI para la automatización de la gestión de vSphere. <https://www.nakivo.com/es/blog/introduction-vmware-vsphere-automation-powercli/>. 2024
28. Daniel Fuentes. RVTools: qué es, cómo descargarlo y para qué sirve en VMware. <https://blogvirtualizado.com/que-es-rvtools-y-por-que-deberiamos-usarlo/>. 2023
29. Nakivo Inc. Los comandos ESXCLI más útiles para su entorno VMware. <https://www.nakivo.com/es/blog/most-useful-esxcli-esxi-shell-commands-vmware-environment/>. 2024
30. Alvaro Miranda. Implementación de vRealize Log Insight 8.4.1. <https://witcherit.com/2021/06/29/implementacion-de-vrealize-log-insight-8-4-1/>. 2021
31. Bacula Systems SA <https://www.baculasystems.com/es/copia-de-seguridad-de-vmware/>. 2024