



Universidad
Zaragoza

Trabajo Fin de Grado

ALTERNATIVAS DE SOFTWARE LIBRE PARA LA CONSOLIDACIÓN DE SERVIDORES EN UNIDADES TÁCTICAS

Autor

Miguel Ángel de la Vega Iges

Director/es

Director académico: D. Marcos Rodríguez Rodríguez.

Director militar: Tte. D. Diego Ray Sánchez.

Centro Universitario de la Defensa-Academia General Militar

Año 2017

RESUMEN

A lo largo de la historia, la información ha sido siempre un recurso crítico que, obtenida y gestionada de la manera apropiada ha llegado a ser decisiva. Por ello, tanto en ámbito civil como militar se desarrollaron los sistemas de información con la finalidad de ayudar a la toma de decisiones.

El presente Trabajo Fin de Grado consiste en la búsqueda de alternativas de software libre para las actuales soluciones licenciadas presentes en los Nodos SIMACET v5 y v4.2, estas soluciones persiguen su robustez y alta disponibilidad de servicios y datos. Para ello se ha realizado un estudio de las necesidades y puntos sensibles de SIMACET a través de entrevistas con sus administradores.

Se ha elaborado un estudio del estado del arte de las tecnologías utilizadas para la consolidación de servidores y almacenamiento con el fin de seleccionar las más adecuadas para el objetivo de esta memoria. Además, se han observado pruebas de rendimiento de dichas tecnologías a modo comparativo entre las diferentes alternativas existentes.

Se ha desarrollado una implementación práctica de la propuesta y se ha comparado el resultado para comprobar si el sistema estaría a la altura o no de las exigencias del actual SIMACET v5.

Por último, se han expuesto las conclusiones y posibles opciones para el futuro.

ABSTRACT

Throughout history, information has always been a critical resource, that obtained and managed in an appropriate manner, has become decisive. For this reason, both in civil and military spheres, systems of information were developed to help decision-making.

The present End of Degree Project consists of the search for free software alternatives for the current licensed solutions present in the SIMACET nodes v5 and v4.2, these solutions pursue their robustness and high availability of services and data. To this end, a study of the needs and sensitive points of SIMACET has been carried out through interviews with its administrators.

A study of the state of the art of the technologies used for the consolidation of servers and storage has been prepared in order to select the most suitable for the purpose of this report. In addition, performance tests of these technologies have been observed in a comparative way between the different existing alternatives.

A practical implementation of the proposal has been developed and the result has been compared to check if the system would be up to the requirements of the current SIMACET v5.

Finally, the conclusions and possible options for the future have been presented.

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer a todo el personal de la Academia General Militar y del Centro Universitario de la Defensa toda la formación, tanto técnica como moral, recibida durante estos años de mi estancia.

Quiero, en particular, agradecer al profesor D. Marcos Rodríguez Rodríguez su labor durante todo el desarrollo de este Trabajo de Fin de Grado, asesorándome para lograr alcanzar todos los objetivos que se han marcado para su correcta finalización.

Además, quiero agradecer a todo el personal del Batallón de Transmisiones II por la experiencia adquirida en las Prácticas Externas, en especial a la compañía de Centros de Transmisiones de Puesto de Mando por su cálido recibimiento. En especial, debo agradecer a su Capitán D. Ricardo Simón Serna la dedicación que ha mostrado para mi integración total en la compañía, siendo un gran ejemplo para mi carrera.

Por último, este trabajo no habría sido posible sin la gran labor del Teniente D. Diego Ray Sánchez, que me ha guiado e instruido durante todo este intenso proceso, ayudándome en todo momento y demostrando que, con dedicación y paciencia, se puede conseguir todo lo que uno se proponga.

ÍNDICE

RESUMEN.....	III
ABSTRACT.....	V
AGRADECIMIENTOS.....	VII
LISTA DE FIGURAS Y TABLAS	X
LISTA DE ACRÓNIMOS	XI
1 INTRODUCCIÓN	1
Objetivo, motivación y alcance del proyecto	1
Ámbito de aplicación	1
Metodología	1
Estructura de la memoria	2
2 ESTADO DEL ARTE.....	3
2.1 Introducción.....	3
2.2 Redundancia y alta disponibilidad de datos.	4
2.2.1 Sistemas RAID	4
RAID 0.....	5
RAID 1.....	5
RAID 5.....	6
RAID 6.....	6
RAID 10.....	7
2.2.2 Sistemas Clúster.....	8
CLASIFICACIÓN	8
Clúster de alto rendimiento HC (High Performance Clusters)	8
Clúster de alta disponibilidad HA (High Availability).....	8
Clúster de alta eficiencia HT (High Throughput)	8
COMPONENTES	8
Nodos.....	9
Sistema Operativo.....	9
Conexión de Red	9
Middleware.....	9
2.3 Consolidación de servidores. Hipervisores y alternativas.	9
2.3.1 Virtualización asistida por hardware	10

2.3.2 Conceptos sobre virtualización	11
Máquina virtual.....	11
Hipervisor.....	12
2.3.3 Modelos de virtualización	13
Virtualización de plataforma o sistema.	13
Virtualización completa.....	14
Emulación	14
Paravirtualización	14
Virtualización a nivel del SO	15
Virtualización a nivel de Kernel	15
Virtualización de recursos.....	15
Virtualización de aplicaciones.....	15
Virtualización de escritorio	15
2.3.4 Ventajas y desventajas de la virtualización	16
3 PRÁCTICA.....	19
3.1 Selección de herramienta de Virtualización	19
3.2 Configuración física del sistema	20
3.3 Configuración lógica del sistema	21
3.4 Funcionamiento del sistema propuesto	24
3.5 Comparativa con el sistema actual.....	26
4 CONCLUSIONES	28
Comentarios personales y líneas futuras de trabajo	28
5 BIBLIOGRAFÍA	30
6 ANEXOS	I
Anexo A - Entrevistas.....	I
Entrevista número 1.....	I
Sargento Especialista Don O.C.N.....	I
Entrevista número 2.....	II
Sargento Especialista Don C.R.E.....	II
Entrevista número 3.....	II
Sargento Especialista Don F.P.M.....	II
Anexo B – Función QFD	III
Anexo C – Comparativa de hipervisores KVM vs Hyper-V VS VMware	V
C.1 Pruebas KVM VS Hyper-V.....	V
C.2 Pruebas Hyper-V VS VMware.....	VIII
Anexo D – Pruebas de rendimiento RAID.....	XI

LISTA DE FIGURAS Y TABLAS

Figura 2.01 Esquema RTP.	4
Figura 2.02 Sistemas de archivos RAID 0 y RAID 1.	5
Figura 2.03 Sistema de archivos RAID 5.	6
Figura 2.04 Sistema de archivos RAID 6.	6
Figura 2.05 Sistema de archivos RAID 0+1.	7
Figura 2.06 Sistema de archivos RAID 1+0.	7
Figura 2.07 Anillos de privilegios en arquitectura x86.	10
Figura 2.08 Anillos de privilegios con soporte de virtualización.	11
Figura 2.09 Máquinas virtuales de hardware.	12
Figura 2.10 Hipervisor hosted.	13
Figura 2.11 Consolidación de servidores.	17
Figura 2.12 Árbol de instantáneas de Workstation	17
Figura 3.2.1 Diagrama de conexión de los equipos.	21
Figura 3.3.1 Sistema de almacenamiento de la práctica.	22
Figura 3.3.2 RAID de discos sincronizado.	22
Figura 3.3.3 Clúster DRBD en interfaz gráfico LCMC.	23
Figura 3.4.1 Esquema general del clúster de Alta Disponibilidad.	24
Figura 3.4.2 Servicios corriendo en nodo <i>Raybian-HP</i> .	25
Figura 3.4.3 Servicios corriendo en nodo <i>Raybian-msi</i> .	25
Figura B.1 Función QFD.	III
Figura C.1.1 Resultado de la primera prueba de KVM.	V
Figura C.1.2 Resultado de la primera prueba de Hyper-V.	VI
Figura C.1.3 Resultado de la segunda prueba de KVM.	VI
Figura C.1.4 Resultado de la segunda prueba de Hyper-V.	VII
Figura C.1.5 Resultado de la tercera prueba de KVM.	VIII
Figura C.1.6 Resultado de la tercera prueba de Hyper-V.	VIII
Figura C.2.1 Resultado de la primera prueba de Hyper-V VS vSphere.	IX
Figura C.2.2 Resultado de la segunda prueba de Hyper-V VS vSphere.	IX
Figura C.2.3 Resultado de la tercera prueba de Hyper-V VS vSphere.	X
Figura D.1 Tiempo de respuesta.	XI
Figura D.2 Rendimiento de lectura de archivos.	XII
Figura D.3 Rendimiento de escritura de archivos.	XII
Tabla 3.1 Características de herramientas de virtualización KVM, Hyper-V y VMware vSphere.	20
Tabla 3.2 Evaluación comparativa del sistema actual VS sistema propuesto.	26

LISTA DE ACRÓNIMOS

CIFS	Common Internet File System
CLR	Common Language Runtime
CPU	Central Processing Unit
DRBD	Distributed Replicated Block Device
GPL	General Public License
GUI	Graphical User Interface
IP	Internet Protocol
JVM	Java Virtual Machine
KVM	Kernel-based Virtual Machine
LCMC	Linux Cluster Management Console
LOS	Line Of Sight
LVM	Logical Volume Manager
MIPS	Microprocessor without Interlocked Pipeline Stages
QFD	Quality Function Deployment
RAID	Redundant Array of Independent Disks
RBA	Red Básica de Área
RTP	Red Táctica Principal
SCTM	Sistema Conjunto de Telecomunicaciones Militares
SIMACET	Sistema de Información para Mando y Control del Ejército de Tierra
SMB	Server Message Block
SO	Sistema Operativo
STONITH	Shoot The Other Node In The Head
TCP	Transmission Control Protocol
TFG	Trabajo de Fin de Grado
VM	Virtual Machine
VPN	Virtual Private Network

1 INTRODUCCIÓN

La redacción de este Trabajo de Fin de Grado se ha realizado durante las Prácticas Externas en el Batallón de Trasmisiones II/1, perteneciente al Regimiento de Trasmisiones 1. Gracias a la colaboración de su personal y medios se ha podido recolectar información de primera mano y de gran utilidad para la elaboración de este proyecto.

OBJETIVO, MOTIVACIÓN Y ALCANCE DEL PROYECTO

El objetivo principal de este Trabajo de Fin de Grado es el de diseñar un sistema, de software libre y coste cero, que consiga llegar a ser una alternativa ante el elevado importe de las licencias de los sistemas de consolidación de servidores utilizados en los Nodos SIMACET.

El prototipo de este sistema se construirá sobre la base de ordenadores personales que, evidentemente, son menos potentes que los servidores que dispone el Nodo. Para el diseño se han definido unos requisitos:

- ✓ Debe estar virtualizado.
- ✓ Debe garantizar alta disponibilidad de datos y procesos.
- ✓ Debe correr sobre software libre.
- ✓ Debe ser capaz de ofrecer un mínimo de servicios que funcionen de forma similar a los que ofrece SIMACET.

Los problemas a abordar a la hora de ofrecer una alternativa competente son la seguridad, la complejidad de administración y el arco de aprendizaje de los operadores frente al coste económico.

El desarrollo habrá finalizado cuando se consiga hacer mínimamente funcional un sistema que reúna las características descritas.

ÁMBITO DE APLICACIÓN

El sistema propuesto está pensado para ser una alternativa a la configuración software actual de los Nodos SIMACET. Estas estaciones están en dotación en todos los Regimientos de Trasmisiones, Brigadas y otras unidades con entidad tipo batallón o menor como son la UTMAAA y FAMET dentro del ámbito del Ejército de Tierra.

METODOLOGÍA

Para la realización de esta memoria se ha seguido un proceso que se inició con la recopilación de información de varias fuentes, de las que se incluyen libros digitales, blogs de tecnologías de información y multitud de recursos web.

Una vez clasificada y seleccionada la información se procedió a aplicarla a la parte práctica. Para analizar los principales requisitos que debía reunir el sistema se

Introducción.

realizaron entrevistas a diferentes administradores del Nodo SIMACET, de las que se han extraído parámetros para mejorar el sistema actual.

Seguidamente se llevaron a cabo diferentes comparativas para justificar la selección de las herramientas utilizadas.

Por último, se realizó la práctica y se procedió a la exposición y explicación de la misma, presentando a la vez las diferentes tecnologías y software utilizados.

ESTRUCTURA DE LA MEMORIA

La memoria está estructurada de la siguiente forma:

- ✓ En la segunda sección se expone la importancia de los sistemas de información para la toma de decisiones y se hace una introducción a los sistemas de redundancia y alta disponibilidad, y a las tecnologías de virtualización existentes.
- ✓ En la tercera sección se analiza todo el proceso de creación y configuración de la práctica, además de una explicación sobre el funcionamiento de la misma para ayudar al lector a su comprensión.
- ✓ En la cuarta sección se exponen las conclusiones sacadas de este Trabajo de Fin de Grado, así como comentarios personales sobre la práctica.

Posteriormente se encuentran los siguientes anexos:

- ✓ En el **Anexo A** se muestran las entrevistas realizadas a los operadores SIMACET.
- ✓ En el **Anexo B** se introducen las propuestas de los operadores en una función QFD y se exponen los resultados.
- ✓ En el **Anexo C** se expone una comparativa entre herramientas de virtualización usadas actualmente en el Ejército de Tierra y la herramienta propuesta para la práctica.
- ✓ Por último, en el **Anexo D** se expone unas gráficas de rendimiento de diferentes tipos de sistema de almacenamiento.



2 ESTADO DEL ARTE

2.1 INTRODUCCIÓN

Gracias a los sistemas de información se puede tener acceso en tiempo casi real a cualquier evento o actualización de una situación que deseemos controlar. Son el medio más importante para proporcionar al Mando las herramientas necesarias para conocer y comprender la situación en el ámbito del Ejército de Tierra. Este hecho es de particular importancia en lo que se refiere al manejo de las operaciones. Poseer la información adecuada, en el formato adecuado, en el momento preciso y con el destinatario correspondiente es esencial para la toma de decisiones y puede determinar el resultado de una operación en curso. De otro modo puede llegar a resultar catastrófico.[1]

Por ello, también hay que asegurar que dicha información sólo es accesible en el ámbito y la clasificación de seguridad adecuada, debiendo tener muy presente la seguridad a la hora de establecer las comunicaciones militares. Las unidades de transmisiones del Ejército de Tierra son las encargadas de montar una red cifrada de telecomunicaciones que permita a la autoridad ejercer el mando y control de las operaciones en un entorno seguro y confiable.

Esta red de telecomunicaciones se compone de tres niveles ordenados de mayor a menor envergadura. El primer nivel se denomina Red Estratégica, Sistema Conjunto de Telecomunicaciones Militares, SCTM¹, de carácter permanente.

En el segundo nivel se encuentra la Red Táctica Principal, RTP, desplegada de forma no permanente. La RTP se compone de:

- ✓ Red Básica de Área, RBA. Red mallada de nodos con radioenlaces LOS² y satélites, extiende servicios a los puestos de mando.
- ✓ Red PAM, extensión de la RBA a través del sistema PROMINAS.

Y, por último, la Red Rádio Combate, RRC, compuesta por los elementos radiados no-LOS en frecuencias HF, VHF y UHF.

¹ SCTM: Sistema Conjunto de Telecomunicaciones Militares.

² LOS: Line of sight, Línea de Visión Directa (LVD).

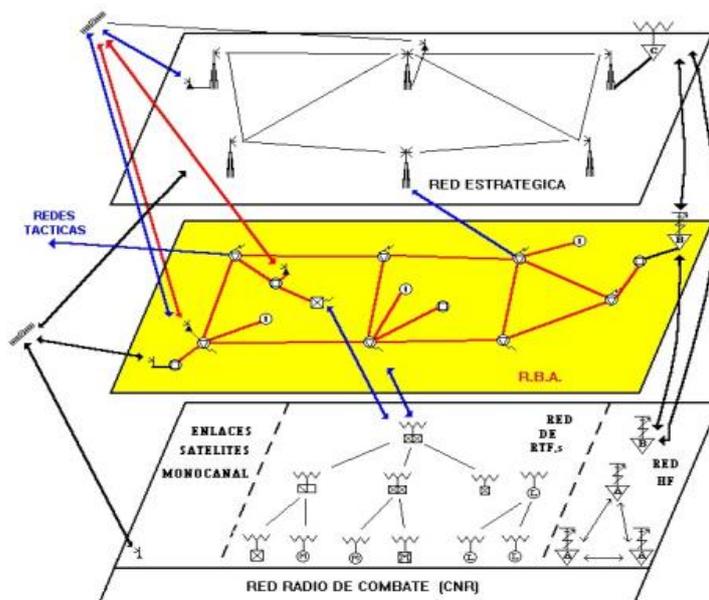


Figura 2.1 Esquema Red de Telecomunicaciones del ET³.

Dentro de esta red de telecomunicaciones militares se despliega el sistema de información denominado Sistema de Mando y Control del Ejército de Tierra (SIMACET).

Dicho sistema se creó con unos objetivos claramente marcados:

- ✓ Visión común del campo de batalla.
- ✓ Sistema de mensajería fiable.
- ✓ Alta supervivencia del sistema.
- ✓ Movilidad de los usuarios.

Para cumplir estos objetivos ofrece a los usuarios una serie de servicios, por ejemplo, un sistema de mensajería intra-teatro, visión común del campo de batalla, correo oficial, sistema de archivos compartidos y otros muchos más. Todo el conjunto facilita el proceso de la toma de decisiones en los diferentes escalones de mando.

Este sistema de información trabaja sobre una base de servidores y almacenamiento que se van a analizar en este trabajo.

2.2 REDUNDANCIA Y ALTA DISPONIBILIDAD DE DATOS.

2.2.1 SISTEMAS RAID

RAID es el acrónimo de “matriz redundante de discos independientes” (Redundant Array of Independent Disks). En esta tecnología, cuanto más alto el número que la define, mayor es la protección contra errores de lectura y pérdida de información en los discos. Con RAID habilitado en un sistema de almacenamiento se pueden conseguir que dos o más discos de almacenamiento funcionen como uno solo más rápido y con más capacidad, o bien como un sistema de almacenamiento con respaldo automático y en tiempo real. Este tipo de almacenamiento se puede habilitar

³ Fuente: PMET OR3-501

tanto por hardware, si la placa base del equipo lo admite, como por software, tanto en Linux como Windows. [2] [3]

Existen varios motivos por los que puede resultar beneficioso utilizar RAID:

- ✓ Porque necesita disponer de un sistema que ofrezca una velocidad de acceso mayor.
- ✓ Para tener un respaldo permanentemente y en tiempo real.
- ✓ Para disponer de ambas características simultáneamente.

RAID 0

Un RAID 0, también conocido como *striping*, utiliza la capacidad de todos los discos del grupo para almacenar la información, repartiéndolos entre los mismos. La mayor ventaja es que ofrece un mejor rendimiento de los datos (Anexo D – Pruebas de rendimiento RAID). Como inconveniente se encuentra la posibilidad de la pérdida total de datos ante cualquier fallo o avería de uno de los discos. [4]

El RAID 0 es la mejor opción a tener en cuenta cuando se prioriza el rendimiento del almacenamiento frente a la seguridad, o cuando el presupuesto es más limitado. [2][3][6]

RAID 1

Un RAID 1, también entendido como *mirroring*, duplica los datos en espejo manteniendo el mismo contenido entre unidades de disco. El sistema operativo lo ve como una sola unidad de almacenamiento. La mayor ventaja es que si se produce un fallo en alguna de las unidades no se perderían los datos. Otra ventaja además de la supervivencia de la información es la posibilidad de un rendimiento mayor en caso de una lectura multiusuario, pudiendo leerse ambos discos simultáneamente. Sin embargo, el coste por almacenaje de datos se duplica, puesto que necesita dos discos para almacenar la misma cantidad de información. [2] [3] [4]

El RAID 1 es una buena opción en un sistema dónde la pérdida de información es inadmisibles, o para sistemas de nivel básico que sólo dispongan de dos discos, como un pequeño servidor de almacenaje. [2] [3] [4]



Figura 2.2 Sistemas de archivos RAID 0 y RAID 1.⁴

⁴ Fuente: Elaboración propia.

Estado del arte.

RAID 5

El RAID 5 es también llamado como distribución con paridad. En esta distribución se realiza una división por bloques de información y se distribuye entre los discos, además se genera un bloque de paridad que, en caso de fallo o avería en alguna de las unidades, se utiliza para la reconstrucción de los datos perdidos, ya que toda la información se encuentra disponible en la suma de la información del resto de las unidades. Sin embargo, el cálculo de la paridad hace que sea más lenta la escritura. Es necesario como mínimo tres discos de almacenamiento y admite sólo fallo en uno de ellos. [2][3][4][5][6]

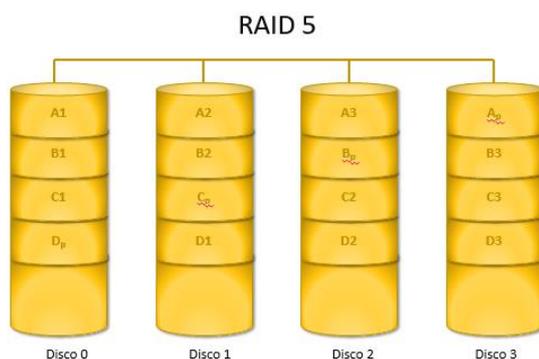


Figura 2.3 Sistema de archivos RAID 5.⁵

RAID 6

Es denominado también como distribuida de doble paridad, siendo similar al RAID 5 en lo que respecta a la distribución de los datos, pero, respecto a la redundancia, se generan dos bloques de paridad que también son distribuidos en los discos. Este sistema admite hasta fallo de dos discos, necesiándose un mínimo de cuatro discos para poder utilizarla. [2] [4]

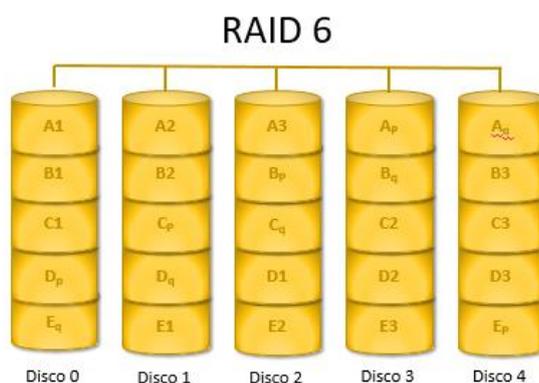


Figura 2.4 Sistema de archivos RAID 6.⁶

⁵ Fuente: Elaboración propia.

⁶ Fuente: Elaboración propia.

RAID 10

Es la combinación de un RAID 0 y un RAID 1 disponiendo de las ventajas de la redundancia y el nivel de rendimiento que ofrecían las dos formas anteriormente descritas. [2][4]

Hay dos posibles combinaciones, el primero es el RAID 0+1, en el que se dividen los datos entre varias unidades y después se duplican en espejo en discos distribuidos idénticamente. [2] [4]

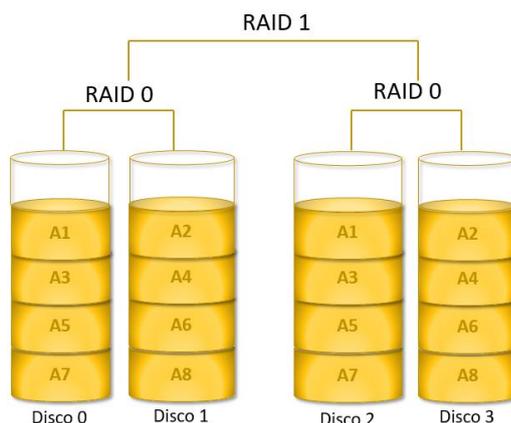


Figura 2.5 Sistema de archivos RAID 0+1.⁷

La segunda combinación posible es el RAID 1+0, en el que los datos se duplican en espejo habiéndose distribuido previamente entre las unidades. [2] [4]

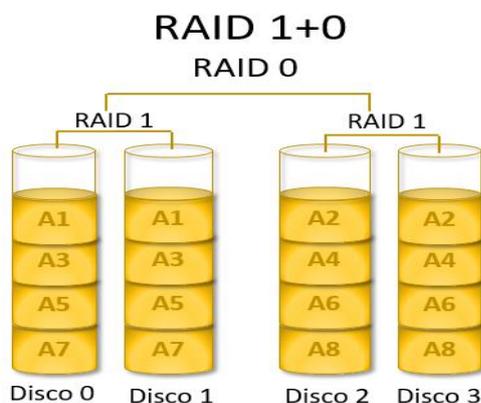


Figura 2.6 Sistema de archivos RAID 1+0.⁸

El RAID 10 es la mejor opción cuando se utilicen aplicaciones que requieran la protección de datos que ofrece el sistema RAID 1 y el rendimiento del RAID 0, un ejemplo son las bases de datos en línea. [2] [4]

En comparación con otros sistemas de archivos con paridad, como el RAID 5 o el RAID 6, ofrece rendimientos superiores durante la reconstrucción de las unidades.

⁷ Fuente: Elaboración propia.

⁸ Fuente: Elaboración propia.

Estado del arte.

Esto es debido a que los datos no necesitan realizar procesos de regeneración de la información de la paridad ya que ésta se encuentra en el disco replicado. [2] [4]

Actualmente, en el Ejército de Tierra, para la consolidación de los servidores de SIMACET se utiliza el sistema RAID 1+0, combinando la seguridad que ofrece el respaldo automático y la velocidad de acceso a los datos necesarios de los usuarios.

2.2.2 SISTEMAS CLÚSTER

Son una unión de servidores configurados de tal forma que trabajan como si fueran uno solo más potente que todos por separado. Para ello deben estar unidos mediante una red de alta velocidad. El resultado esperado del sistema, dependiendo de la configuración que se establezca, es una combinación de los siguientes servicios:[7]

- ✓ Alto rendimiento.
- ✓ Alta disponibilidad.
- ✓ Equilibrio de carga.
- ✓ Escalabilidad.

CLASIFICACIÓN

En función de sus características podemos clasificarlos en: [7]

Clúster de alto rendimiento HC (High Performance Clusters)

Estos sistemas son capaces de ejecutar tareas que requieren gran capacidad de cálculo o del uso de grandes cantidades de memoria compartida. Mientras estén realizando este tipo de tareas, los recursos del clúster son utilizados casi en exclusiva.

Clúster de alta disponibilidad HA (High Availability)

Este tipo de sistema se monta para ofrecer disponibilidad y confiabilidad a los servicios. Para conseguirlo, se utiliza hardware duplicado, así, aunque se produzca una avería en un componente, siempre habrá otro que pueda realizar el mismo trabajo. Además, incorporan software de detección y recuperación ante errores, con objeto de ofrecer aún más fiabilidad.

Clúster de alta eficiencia HT (High Throughput)

En este tipo de sistemas el objetivo es que se puedan ejecutar el mayor número de tareas en el menor tiempo posible, siempre y cuando sean tareas individuales cuyos datos no tengan interdependencia.

COMPONENTES

Para que el sistema funcione es necesario un interfaz de manejo de clúster, el cual se encarga de intermediar entre el administrador y los procesos, repartiendo la carga entre los equipos. Sin embargo, no es necesario que todos los equipos dispongan del mismo Hardware y SO (si así fuera se denominaría clúster heterogéneo). [7]

Los componentes de un clúster, entre otros, son: [7]

- ✓ Nodos (Ordenadores o servidores)

- ✓ Sistema Operativo
- ✓ Conexión de Red
- ✓ Middleware (Interfaz entre el usuario y el sistema operativo)
- ✓ Protocolos de comunicación y servicio
- ✓ Aplicaciones

Nodos

Puede ser cualquier tipo de máquina como ordenadores de escritorio o servidores. [7]

Sistema Operativo

Deben tener entorno multiusuario. Algunos ejemplos de sistemas operativos para clúster son, "Microsoft Windows Server 2008", o las alternativas para un sistema Linux/Unix como "Debian 9.1 Stretch" o "Solaris". [7]

Conexión de Red

Se pueden interconectar con conexiones Ethernet o sistemas de alta velocidad como Fast Ethernet, Gigabit Ethernet, Infiniband, SCI, etc. [7]

Middleware

Es el software que actúa entre el SO y las aplicaciones. Provee una única interfaz de acceso al sistema, llamada "Single System Image", que optimiza el sistema además de ofrecer herramientas de mantenimiento para procesos como migraciones, tolerancia de fallos o balanceo de carga. [7]

También se encarga de administrar la escalabilidad del sistema ya que posee la capacidad de detectar nuevas máquinas y añadirlas al grupo. [7]

Por tanto, este tipo de sistemas ofrecen una gran fiabilidad ante errores, ya que para una parada completa del proceso deberían pararse todas las máquinas que componen el clúster. Es la opción más competente si se necesita ampliar el sistema, ya que se pueden añadir tantos equipos como sea necesario. [7]

2.3 CONSOLIDACIÓN DE SERVIDORES. HIPERVISORES Y ALTERNATIVAS.

Hoy día la virtualización se ha convertido en una solución muy empleada por las empresas a nivel mundial, ofreciendo gran número de ventajas y buenos resultados. Sin embargo, no es una tecnología nueva, sino que lleva siendo utilizada más de cuarenta años, aunque no explotada tan eficientemente como en la actualidad, siendo la consolidación de servidores y la virtualización de SO las aplicaciones más interesantes que ofrece.[8]

La virtualización es el efecto de abstraer los recursos de un computador, proporcionando acceso lógico a los recursos físicos. [8]

Esta técnica aporta ventajas y posibilidades únicas. Permite ahorrar costes en casi todos los ámbitos de la administración de sistemas, desde la instalación y

Estado del arte.

configuración de computadoras hasta los procesos de respaldo, monitorización, gestión y administración de la infraestructura. Gracias a ella podemos reducir el número de servidores físicos necesarios y el porcentaje no utilizado de los recursos de los que disponen, aumentando así la eficiencia energética. También nos ofrece la posibilidad de centralizar y automatizar procesos cuya administración normalmente consumiría más tiempo, pudiendo aprovisionar y migrar máquinas virtuales de una forma rápida y fiable, y manteniendo el nivel de servicio requerido. [8]

2.3.1 VIRTUALIZACIÓN ASISTIDA POR HARDWARE

La virtualización asistida por hardware hace uso de circuitería en la CPU y chips controladores que mejoran la ejecución y rendimiento de múltiples SO en máquinas virtuales. Gracias a esta tecnología podemos implementar virtualización pura sin necesidad de modificar los SO invitados, como hace el software XEN en la paravirtualización, y sin necesidad de emular las instrucciones cuyo procesamiento resulta problemático, como hacen algunos de los software más conocidos y utilizados, como VMware Workstation. El rendimiento es notablemente superior como consecuencia. [8]

El origen de esta tecnología está en los problemas aparecidos en la arquitectura x86 por algunas de las instrucciones de procesamiento cuando las técnicas de virtualización quieren ser aplicadas. El problema surgía cuando instrucciones pertenecientes al modo privilegiado no podían ser capturadas, e incluso devolvían diferentes valores dependiendo del nivel de privilegios de quien originaba la llamada. [8]

Para entender el concepto anterior es necesario introducir los **anillos de protección o privilegios**. La arquitectura x86 dispone de cuatro anillos de protección, desde el nivel con mayor privilegio donde se encuentra el núcleo del SO, que es el nivel 0, al nivel 3 con menos privilegios y donde corren las aplicaciones. Los niveles 1 y 2 albergan los controladores de los dispositivos. [8]

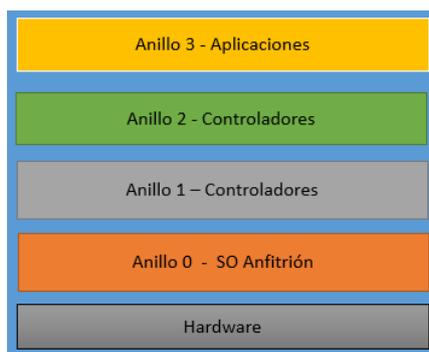


Figura 2.07 Anillos de privilegios en arquitectura x86.⁹

Las empresas más conocidas en el mundo de los microprocesadores, Intel y AMD, implementan en sus procesadores tecnologías o soluciones que permiten realizar virtualización completa y usar cualquier SO invitado en las máquinas virtuales.

⁹ Fuente: Elaboración propia.

Además, ofrecen instrucciones de la familia x86, entendiéndolo como las nativas 32bits x86 y AMD64 como su extensión a 64 bits, para que un hipervisor controle el acceso de hardware del nivel 0 de privilegios. De esta forma se crea un “anillo -1” para que el SO invitado pueda ejecutar operaciones de nivel 0 de forma nativa sin afectar al resto de invitados o al SO anfitrión. [8]



Figura 2.08 Anillos de privilegios con soporte de virtualización.¹⁰

2.3.2 CONCEPTOS SOBRE VIRTUALIZACIÓN

Antes de continuar es imprescindible conocer dos conceptos que son fundamentales y que actúan como base a los modelos de virtualización existentes. Estos son la **máquina virtual** y el **hipervisor**, necesarios para entender el fundamento de las principales técnicas que se presentarán posteriormente. [8]

Es difícil comprender el funcionamiento de estas técnicas sin saber qué es una máquina virtual, ya sea de sistema o de aplicación. El concepto de hipervisor o monitor es clave debido a que es el aspecto diferenciador entre las técnicas de virtualización completa y paravirtualización, actualmente los modelos más extendidos. [8]

MÁQUINA VIRTUAL

Según las características y funcionalidades de la propia máquina podemos distinguir entre máquina virtual de hardware (también conocidas como de sistema) o máquina virtual de proceso (también conocidas como de aplicación). [8][9]

Las **máquinas virtuales de hardware** son aquellas que funcionan paralelamente sobre una computadora física llamada "host" o anfitrión, de tal forma que pueden acceder y hacer uso de los recursos físicos abstraídos de la misma. Éstas creen que poseen dichos recursos hardware de forma exclusiva cuando en realidad lo hace de una forma virtual. [8][9]

¹⁰ Fuente: Elaboración propia.

Estado del arte.

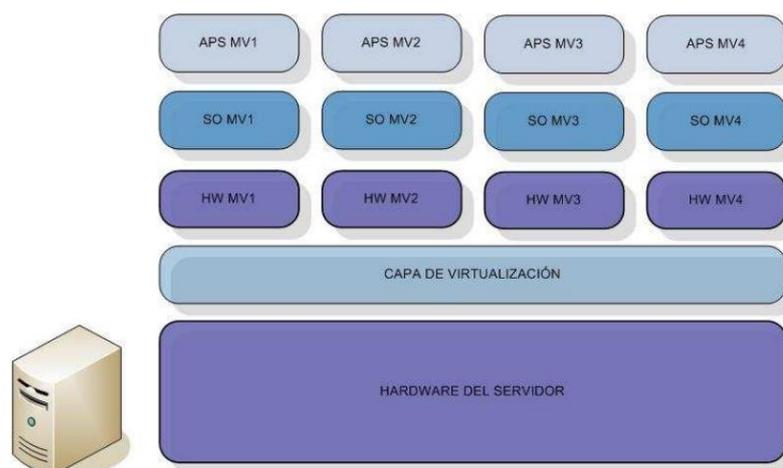


Figura 2.09 Máquinas virtuales de hardware.¹¹

Este tipo de máquinas es muy útil, no requieren de virtualización asistida por hardware, y ofrece varias características como la posibilidad de que coexistan varios SO, consolidación de servidores o incluso para testear proyectos, ya que permiten utilizar diferentes arquitecturas de instrucciones.

Las **máquinas virtuales de proceso** tienen como objetivo la portabilidad de código, para ello independizan el código fuente e intermedio de un programa del código máquina dependiente del HW. Se denominan códigos semi-interpretados, a diferencia de los códigos compilados tal como la familia C. Un programa compilado en C para una arquitectura MIPS no es portable a una arquitectura x86, pero en cambio un software semi-compilado/interpretado en Java sí es portable inter-plataformas. Ejemplos son JVM (Java Virtual Machine), de Sun Microsystems, y CLR (Common Language Runtime), de Microsoft. [8][9]

HIPERVISOR

Es un monitor de máquinas virtuales que se inicia automáticamente durante el arranque, antes de las máquinas, y que suele correr justo encima del hardware (también conocido como Baremetal). Sin embargo, no es necesario su uso en todas las soluciones de virtualización existentes, sólo se utiliza en paravirtualización y virtualización completa.[8]

El hipervisor ofrece al usuario una serie de funciones que permiten que las máquinas virtuales funcionen correctamente. Se encarga de identificar, captar, manejar y responder a las operaciones de la CPU e instrucciones privilegiadas o protegidas emitidas por las máquinas virtuales. Además, maneja el encolado, envío y devolución de resultados de las peticiones de acceso a los recursos de la máquina anfitriona. [8]

¹¹Fuente: http://www.adminso.es/images/6/6d/Eugenio_cap1.pdf. Página 25.

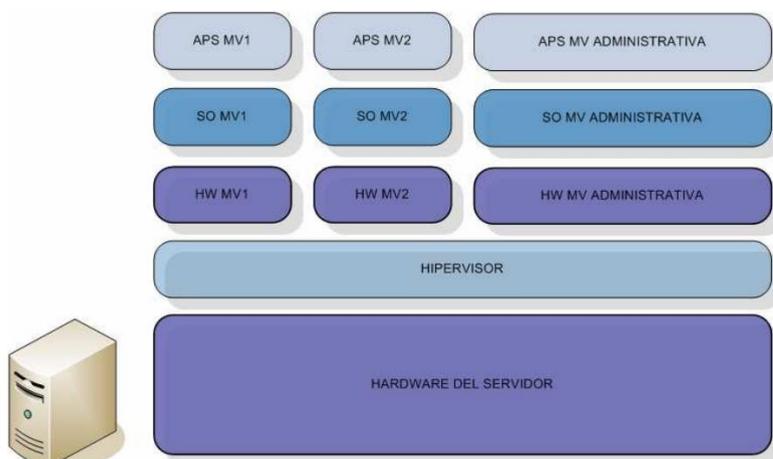


Figura 2.10 Hipervisor hosted.¹²

Como se puede observar en la **Figura 2.10**, el hipervisor corre entre el hardware y los distintos SO, tanto de máquinas virtuales como la máquina host. Así puede cumplir con el objetivo de administrar las instancias de las máquinas virtuales comunicándose con el SO anfitrión. Para ello cuenta con herramientas de gestión y monitorización, además de las que el administrador desee añadir.

En los modelos de virtualización completa y paravirtualización se utiliza siempre, independientemente de si la máquina tiene hardware con soporte de virtualización específico. En el modelo de paravirtualización se introducen cambios en los SO invitados que les permiten comunicación directa con el hipervisor, mejorando así el rendimiento. Sin embargo, cualquier modelo basado en hipervisor sólo podrá gestionar máquinas virtuales con SO que utilicen los mismos juegos de instrucciones que el SO de la máquina física. [8]

2.3.3 MODELOS DE VIRTUALIZACIÓN

Para poder diferenciar entre los distintos modelos que existen debemos saber que la clasificación se basa en dos conceptos, el recurso virtual que se abstrae, y la aplicación, sistema operativo, o máquina que, virtualizado, hace uso de dicho recurso. En base a las diferentes uniones de ambos conceptos se puede distinguir de un modelo u otro. [8]

VIRTUALIZACIÓN DE PLATAFORMA O SISTEMA.

En este modelo, el recurso abstraído es una máquina completa. Las instancias de cada invitado se efectúan de manera independiente a las del resto, de esta forma las máquinas creen que los recursos le pertenecen de manera exclusiva y no se ven entre ellas, desconociendo que comparten recursos. Este aspecto es fundamental para la seguridad en la capa de virtualización. [8]

De los tipos existentes es el más interesante, ya que es el utilizado para realizar la **consolidación de servidores**. Esto, a efectos prácticos, puede verse como el

¹² http://www.adminso.es/images/6/6d/Eugenio_cap1.pdf. Página 27.

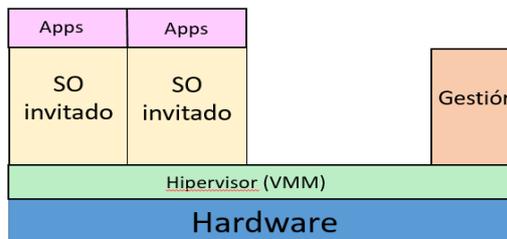
Estado del arte.

particionado, de manera virtual, de un servidor físico en distintos servidores dedicados. Así cada una de las máquinas puede ser asignada a un servicio distinto, haciendo uso de manera común de los recursos del hardware anfitrión y ofreciendo la ventaja del aislamiento total entre servicios en caso de errores o ataques. [8]

Dentro de la virtualización de plataforma también se puede diferenciar entre diferentes modelos

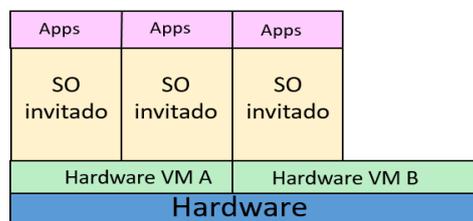
Virtualización completa

Este tipo utiliza un hipervisor (explicado anteriormente) entre los SO invitados y el SO anfitrión. Además, puede incluir soporte hardware específico para virtualización para aumentar el rendimiento. Algunos ejemplos que utilizan este modelo son: Oracle VM, VMware ESX server, XenServer o Hyper-V. [8]



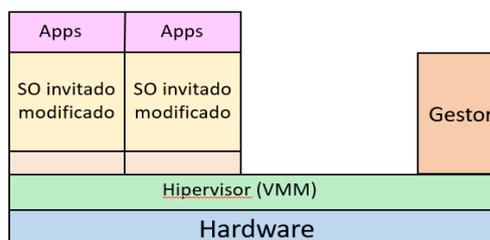
Emulación

En este tipo se replica una máquina completa, incluyendo procesador, memorias, periféricos hardware. Permite la ejecución de cualquier tipo de SO y aplicaciones. Algunos ejemplos son VirtualPC o MESS. [8]



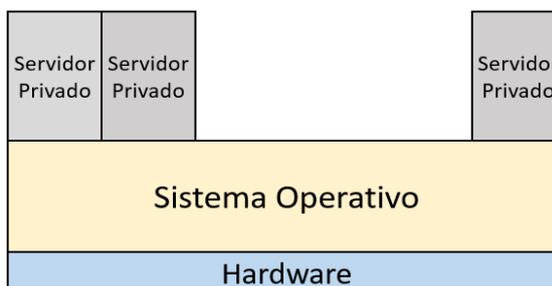
Paravirtualización

Es similar a la virtualización completa ya que tiene una capa intermedia de hipervisor, sin embargo, en este caso se introducen modificaciones en los SO invitados para cooperen en la virtualización. Esto implica que las máquinas virtuales son conscientes del proceso, pero se elimina la necesidad de capturar, por parte del hipervisor, instrucciones privilegiadas que puedan resultar conflictivas. De esta forma se consigue un aumento del rendimiento casi similar al de un sistema no virtualizado. Además, puede contar con soporte hardware específico para virtualización añadiendo un plus de rendimiento. Las soluciones más conocidas son Xen, Oracle VM y Sun Xvm Server. [8]



Virtualización a nivel del SO

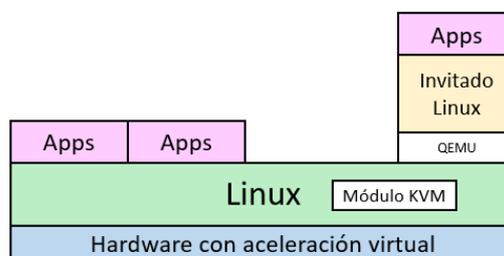
En este modelo se virtualizan los servidores sobre el propio SO anfitrión sin necesidad de introducir una capa de virtualización. Simplemente aísla los servidores entre sí compartiendo SO, ofrece rendimientos similares a sistemas no virtualizados, aunque requiere cambios en el núcleo del SO. Al



compartir el mismo núcleo, las máquinas no pueden usar un SO diferente al anfitrión, aunque sí distintas versiones o distribuciones del mismo. Algunas soluciones representativas son OpenVZ, Solaris Containers o Linux V-Server. [8]

Virtualización a nivel de Kernel

Para implementar este modelo es necesario convertir el núcleo Linux en un hipervisor mediante un módulo, el cual permite ejecutar máquinas virtuales a la vez que otras instancias de SO en el espacio de usuario del núcleo Linux anfitrión. Los SO invitados deben ser compatibles con el hardware de la máquina anfitrión. Existen dos soluciones que destacan en este modelo, KVM (Kernel Virtual Machine) y User-mode Linux. [8]



VIRTUALIZACIÓN DE RECURSOS

En este caso se abstraen los recursos de hardware de una computadora, como puede ser la tarjeta de red, almacenamientos principal o secundario y los dispositivos de entrada y salida. Existen varios ejemplos conocidos de virtualización de recursos como pueden ser los sistemas RAID de almacenamiento, las redes VPN (Virtual Private Network), LVM (Logical Volume Manager) o los sistemas de almacenamiento en red NAS (Network-Attached Storage). [8]

VIRTUALIZACIÓN DE APLICACIONES

Las aplicaciones virtualizadas están encapsuladas sobre el SO de forma que no necesitan estar instaladas en la máquina anfitrión para poder ejecutarse. Se ejecutan dentro de un entorno virtual aislado, que contiene a la aplicación y al propio entorno y configuraciones, que no modifica nada del sistema local. Esta característica le permite ser portable y compatible con cualquier sistema. Algunos ejemplos son Wine, JVM (Java Virtual Machine) o CLR (Common Language Runtime). [8]

VIRTUALIZACIÓN DE ESCRITORIO

Esta técnica permite al usuario manejar el escritorio de una máquina de forma remota pudiendo acceder a aplicaciones o datos sin estar en el mismo emplazamiento.

Estado del arte.

Para ello el escritorio es almacenado en un servidor central en vez de en el ordenador local. Es encapsulado y entregado, así el usuario puede acceder desde distintos dispositivos. Algunos ejemplos de soluciones que trabajan con virtualización de escritorio son Sun VDI, Wyse Technology, VMware View o XenDesktop. [8]

2.3.4 VENTAJAS Y DESVENTAJAS DE LA VIRTUALIZACIÓN

Una vez conocidas las diversas técnicas de virtualización se pueden ver cuales son los beneficios y pormenores de utilización de las mismas.

Quizá una de las mejoras más importantes que ofrece la virtualización es la **tasa de uso** de las máquinas físicas que ofrece. Sin usar esta técnica se podía utilizar unos porcentajes del 15% o 20% de la capacidad de computación, lo cual dejaba un amplio margen de desuso, lo que implica un gasto energético innecesario, ya que, aunque no se utilice todo el potencial, el consumo eléctrico es casi el mismo. Esto se traduce en una mejora en eficiencia energética, reducción de costes en hardware y costes menores de administración de los servidores. [8][10][11]

Además, con el crecimiento de las tecnologías de información, se ha producido un cambio entre las empresas para adaptarse a los nuevos modelos de negocio basados en software y automatizados, haciendo que se pase del almacenamiento físico en papel al almacenamiento masivo de la información de manera digital. Esta situación requiere nuevos estilos de almacenamiento como los ofrecidos por la **virtualización de almacenamiento**, que permite una abstracción completa del almacenamiento lógico sobre el físico. Así se consigue reducir el espacio de los data-center con la consecuente reducción de los costes y del consumo energético. [8][10][11]

Otra ventaja reside en la gran reducción en costes de **administración de sistemas**, donde, gracias a la virtualización, se consigue una monitorización simplificada y centralizada, provisión de máquinas de forma automática, simplificación en los procesos de copia de seguridad y restauración y aislamiento entre servicios. [8][10][11]

Pero lo más interesante en lo que atañe al campo de este trabajo de fin de grado es una ventaja derivada de todas las anteriores, la **consolidación de servidores, Figura 2.12**. Consiste en la reducción del número de máquinas físicas aumentando su tasa de utilización. Al hacerlo, se permite usar despliegues fácilmente escalables, gracias a la modularidad que ofrece, y centralizar y simplificar la administración. [8][10][11]

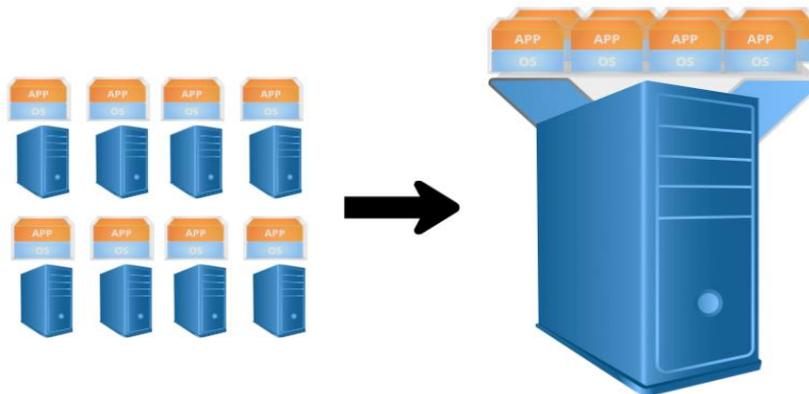


Figura 2.11 Consolidación de servidores.¹³

Sin embargo, a **nivel de servicio**, la característica más importante para el usuario reside en la robustez que ofrece la virtualización. Gracias a la capacidad de redundancia y replicación que se consigue con la consolidación de servidores, el sistema está dotado de una alta disponibilidad y un rendimiento mayor que sin aplicar estas técnicas.

Por último, cabe destacar la utilidad que ofrece respecto a la **escalabilidad** del sistema o la mejora de las políticas de **puesta en marcha, copias de seguridad y recuperación**. La capacidad de crear snapshots, **Figura 2.12**, o instantáneas de las máquinas virtuales nos permite recuperar el sistema con facilidad (pudiendo volver a un estado anterior), reduciendo el proceso a copiar y pegar dichas copias de seguridad, o aumentar el número de equipos desde una máquina virtual pre-configurada (instalando la misma en otras máquinas). Esta utilidad permite además disponer de un entorno para hacer pruebas con fácil recuperación en caso de errores o de introducir modificaciones. [8]

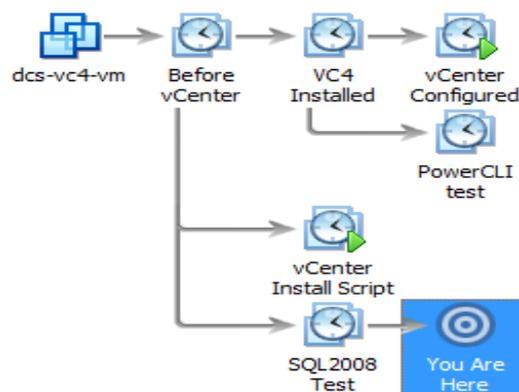


Figura 2.12 Árbol de instantáneas de Workstation¹⁴

Por otro lado, la virtualización tiene una serie de desventajas de las cuales la más evidente es que ofrecen un **rendimiento menor** frente a los sistemas tradicionales,

¹³ Fuente: Elaboración propia.

¹⁴ Fuente: Elaboración propia.

Estado del arte.

(teniendo en cuenta la comparación de una sola máquina virtual frente a una máquina física) debido a que el hardware no es exclusivo de cada máquina, y aunque lo fuese, cuenta con una capa intermedia que utiliza parte de los recursos de computación. Incluso se puede llegar a una situación de desaprovechamiento del rendimiento si se poseen excesivas máquinas virtuales por culpa de una mala planificación. Además, hay que realizar un **aprendizaje previo** por parte de los administradores para familiarizarse con los entornos virtuales.

En cuanto a **supervivencia del sistema**, se puede comprobar que ofrece mayor resistencia a errores, pero existe el riesgo de que todas las máquinas virtuales caigan si se produce una avería en la máquina anfitrión, situación que puede evitarse creando un clúster de servidores anfitriones.

3 PRÁCTICA

Gracias a las entrevistas realizadas con los operadores del Nodo SIMACET, **Anexo A**, se han recogido varios factores que deberían mejorarse. Las opiniones se han introducido en una herramienta de calidad, llamada *casa de la calidad*, **Anexo B**, que es capaz de determinar la importancia e impacto de las acciones de mejora propuestas por los administradores.

Resultado del análisis se ha llegado a la conclusión de la necesidad de hacer uso de las tecnologías de **virtualización, clúster de alta disponibilidad** y de mantener el actual **sistema de almacenamiento RAID 0+1**.

3.1 SELECCIÓN DE HERRAMIENTA DE VIRTUALIZACIÓN

Para la elección de la herramienta de virtualización se ha realizado una comparativa entre tres opciones posibles, dos de ellas ya están implementadas en el Ejército de Tierra en este momento, Microsoft Hyper-V utilizado en los Nodos transición 4.2 y VMware ESXi vSphere en los nuevos Nodos v5. Ambas soluciones son de pago, por lo que se propone la alternativa gratuita basada en KVM, incluida en los SO Linux.

Las tres herramientas ofrecen características similares:

	Hyper-V	VMware vSphere	KVM
Desarrollador	Microsoft	VMware	Red Hat
CPU invitada	X86-64	X86-64	X86-64
Modo de operación	Virtualización, Intel VT-x, AMD-V	Virtualización, Intel VT-x, AMD-V	Intel VT-x, AMD-V
Soporte de Drivers invitados	Si	Si	Si
Soporte comercial	Si	Si	Si
Consolidación de servidores	Si	Si	Si
Toma de Snapshots	Si	Si	Si
Aceleración 3D	Si	Si (a partir de 4.0)	Si

Práctica.

Migración de MV en "caliente"	Si	Si	Si
-------------------------------	----	----	----

Tabla 3.1 Características de herramientas de virtualización KVM, Hyper-V y VMware vSphere.¹⁵

Como se puede observar en la tabla, las tres herramientas ofrecen las mismas funcionalidades de cara a esta práctica. Por tanto, y al margen del rendimiento que ofrece cada una, se podría afirmar que son igual de válidas.

En cuanto al rendimiento, **Anexo C**, se han estudiado pruebas de rendimiento a las que han sido sometidas las tres opciones, demostrando características similares en cuanto a la ejecución de máquinas virtuales se refiere, con vSphere 5.5 como alternativa de mejor rendimiento.

Sin embargo, el apartado del coste es determinante.

En el caso de Hyper-V de Microsoft, es necesario adquirir dos licencias:

- ✓ Windows Server 2012 R2 Datacenter: 4307.68 € (Licencia válida para dos procesadores, dos licencias por Nodo).
- ✓ System Center 2012 R2: 3231€ (Necesaria una licencia para cada Nodo).

Para cada Nodo SIMACET de Pequeña Unidad son necesarios 11846.36 € en concepto de licencias Microsoft.

La alternativa VMware también requiere la adquisición de dos tipos de licencias:

- ✓ vSphere 5.5 Enterprise Plus: 1602.70 € (Licencia válida para un procesador, cuatro licencias por Nodo).
- ✓ Vcenter Enterprise: 3158.90 € (Necesaria una licencia para cada Nodo).

Para cada Nodo SIMACET de Pequeña Unidad son necesarios 9569.7 € en concepto de licencias de VMware.

La opción seleccionada para la práctica, **KVM**, es de licencia GNU GPL¹⁶ de la casa Open Virtualization Alliance, completamente gratuita, con las mismas características y con rendimiento similar a las dos alternativas usadas en el Ejército de Tierra.

3.2 CONFIGURACIÓN FÍSICA DEL SISTEMA

Se propone el uso de un clúster de alta disponibilidad HA, tanto de datos como de procesos, para aumentar la supervivencia del sistema ante errores, con el fin de mantener en todo lo posible los servicios ofrecidos. Para el desarrollo práctico se utilizarán tres ordenadores portátiles interconectados a través de un switch y un disco duro externo, **Figura 3.2.1**.

¹⁵ Fuente: Elaboración propia.

¹⁶ GPL: Global Public License.

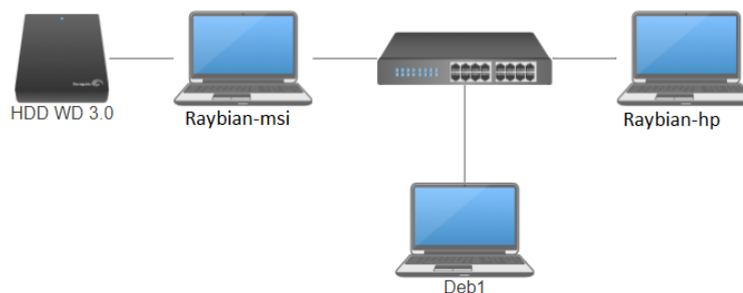


Figura 3.2.1 Diagrama de conexión de los equipos.¹⁷

Las características técnicas de los equipos son las siguientes:

Equipo portátil MSI “RayBian-msi”:

- ✓ Procesador: Intel® Core™i7-5700HQ CPU @ 3.30GHz
- ✓ Memoria RAM: 16GB DDR4.
- ✓ HDD: 1TB + 120GB SSD.
- ✓ SO: Debian 9.

Equipo portátil TOSHIBA “Deb1”:

- ✓ Procesador: Intel® Core™i5-3337U CPU @ 1.80GHz
- ✓ Memoria RAM: 6GB.
- ✓ HDD: 750 GB DDR3.
- ✓ SO: Debian 9.

Equipo portátil HP “Raybian-HP”:

- ✓ Procesador: Intel® Core™i5 CPU @ 1.80GHz.
- ✓ Memoria RAM: 4GB DDR3.
- ✓ HDD: 750 GB.
- ✓ SO: Debian 9.

Disco duro externo Western Digital:

- ✓ Capacidad: 1TB.
- ✓ Conexión: USB 3.0.

Para la interconexión de los equipos se ha utilizado un switch y cables de red Ethernet.

3.3 CONFIGURACIÓN LÓGICA DEL SISTEMA

En cuanto al almacenamiento y a pesar de que, en las pruebas de rendimiento, **Anexo D**, es notable el buen funcionamiento del RAID 10, se va a utilizar sólo el RAID 1 por no disponer de más medios para la práctica. Esta decisión es suficiente ya que la característica buscada para el almacenamiento es la de redundancia de datos en caso de errores en disco.

¹⁷ Fuente: Elaboración propia.

Práctica.

Además, para asegurar la disponibilidad, el RAID 1 estará conectado en clúster con otro disco más que servirá como respaldo, **Figura 3.3.1**.

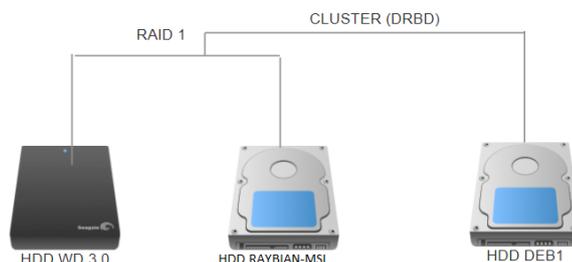


Figura 3.3.1 Sistema de almacenamiento de la práctica.¹⁸

Para la configuración del sistema RAID se utiliza la herramienta nativa LVM¹⁹ con la que se crearán particiones tipo LVM en los discos duros de los equipos *RayBian-msi*, *Deb1* y *WD*. Se crearán los *grupos de volúmenes* y *volúmenes lógicos* necesarios y se activará la característica *mirror* (RAID 1).

Deben crearse volúmenes lógicos idénticos en los tres discos que se utilicen en el clúster, debido a que estarán sincronizados entre ellos. Si bien lo ideal sería crear un grupo de volúmenes independiente para datos e imágenes de disco de máquinas virtuales, en el despliegue se usará un solo grupo de volúmenes, *datoscluster*, con un único volumen lógico, *datos*.

LV	VG	Attr	LSize	Pool	Origin	Data%	Meta%	Move	Log	Cpy%Sync	Convert	Devices
datos	datoscluster	rwi-aor--	80,00g							100,00		datos_rimage_0(0),datos_rimage_1(0)
[datos_rimage_0]	datoscluster	iwi-aor--	80,00g									/dev/sda3(0)
[datos_rimage_1]	datoscluster	iwi-aor--	80,00g									/dev/sdc6(1)
[datos_rmeta_0]	datoscluster	ewi-aor--	4,00m									/dev/sda3(20480)
[datos_rmeta_1]	datoscluster	ewi-aor--	4,00m									/dev/sdc6(0)
datosmsi-lv	datosmsi-vg	-wi-ao---	652,05g									/dev/sdb1(0)
rootmsi	raybianmsi-vg	-wi-ao---	119,12g									/dev/sda4(0)
rootwd-lv	rootwd-vg	-wi-a----	27,94g									/dev/sdc7(0)
WinGen-lv	virtual-vg	-wi-a----	20,00g									/dev/sdb5(0)

Figura 3.3.2 RAID de discos sincronizado.²⁰

Una vez que se tienen los discos particionados de la forma deseada y se ha configurado el RAID, **Figura 3.3.2**, se procederá a crear y configurar el clúster de alta disponibilidad, **Figura 3.3.3**. Para ello se hará uso de la Consola de Administración de Clústers de Linux LCMC²¹. Este software es un interfaz gráfico de usuario (GUI²²) que configura, gestiona y monitoriza los clústers. Para ello utiliza varios componentes:

- ✓ Pacemaker: Administrador de recursos de clúster, encargado de crear y monitorizar el clúster de alta disponibilidad entre los servidores. En esencia permite activar y desactivar servicios y recursos, como IPs, de un nodo a otro del clúster atendiendo a errores y preferencias. Usa Corosync como elemento de mensajería de eventos entre los nodos.

¹⁸ Fuente: elaboración propia.

¹⁹ Logical Volume Manager.

²⁰ Fuente: elaboración propia.

²¹ Linux Cluster Management Console.

²² Graphic User Interface.

- ✓ Corosync: Se encarga de proporcionar la comunicación entre los nodos del sistema y dar la información necesaria para el mantenimiento del clúster a Pacemaker
- ✓ STONITH²³: Es el responsable de evitar que equipos que han quedado fuera del clúster por demostrar una disfunción sigan accediendo a los recursos de este, degradando en nuestro caso, los datos gestionados por DRBD.
- ✓ DRBD: Se encarga de crear un clúster de datos (por TCP/IP²⁴) para dar respaldo continuo.
- ✓ SAMBA: Servicio de ficheros e impresoras compartidos en red que usa el protocolo SMB/CIFS²⁵

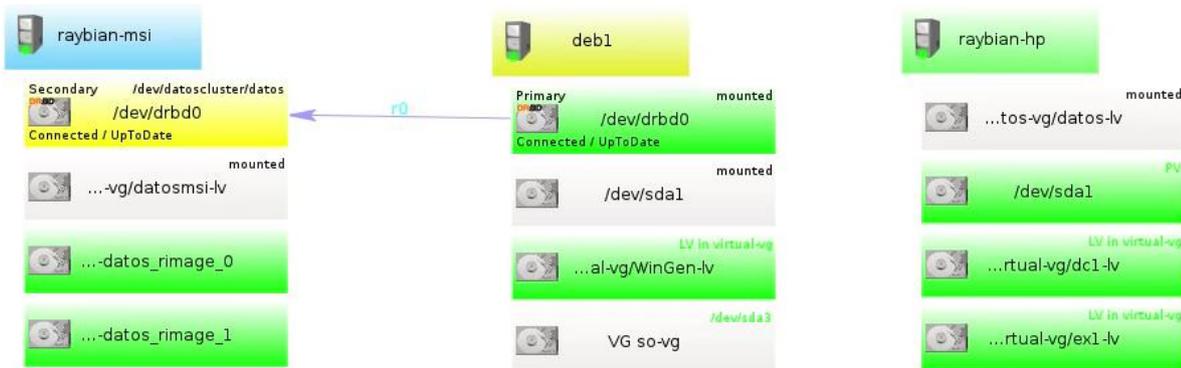


Figura 3.3.3 Clúster DRBD en interfaz gráfico LCMC.²⁶

La gran ventaja que ofrece LCMC es facilitar la configuración de todo el sistema a través de su interfaz gráfico, **Figura 3.3.3**, en lugar de tener que utilizar la línea de comandos. Esto es positivo para los posibles administradores al reducir la cantidad de conocimientos previos sobre Linux y mejorar el arco de aprendizaje. Además, ofrece una representación muy intuitiva sobre el estado de los servicios y recursos.

Finalizada la configuración lógica, se montará una máquina virtual con SO Windows 10 y un servidor web Apache, simulando el comportamiento de cualquiera de los servicios que puede correr un Nodo SIMACET (Mapa de situación, mensajería oficial, correo interno, archivos compartidos, etc.).

Estos servicios, en el Nodo SIMACET, correrían sobre máquinas virtuales con SO Windows Server 2008 y Windows Server 2012, por lo que tendrían el mismo comportamiento dentro del clúster de la práctica que el servidor web y la máquina virtual utilizadas.

Cabe señalar que el servicio Apache corre desde el servidor físico y no desde el virtualizado a modo de ejemplo de las posibilidades de Pacemaker.

²³ STONITH: Acrónimo en inglés de Shoot-The-Other-Node-In-The-Head.

²⁴ TCP/IP: Transmission Control Protocol/Internet Protocol.

²⁵ SMB/CIFS: Server Message Block/Common Internet File System.

²⁶ Fuente: Elaboración propia.

Práctica.

3.4 FUNCIONAMIENTO DEL SISTEMA PROPUESTO

Configurada la práctica se va a proceder a explicar el funcionamiento del clúster.

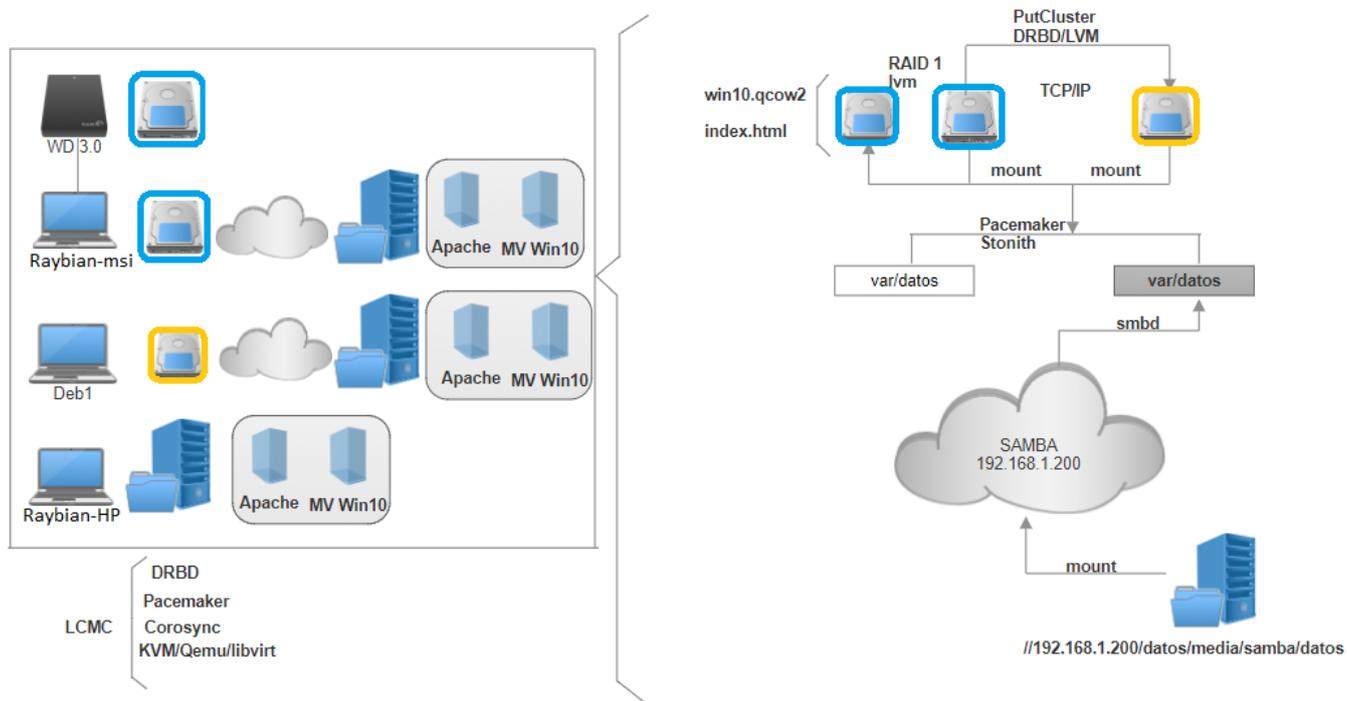


Figura 3.4.1 Esquema general del clúster de Alta Disponibilidad.²⁷

Pacemaker va a controlar en todo momento el clúster, asegurando la disponibilidad de máquinas virtuales y servicios. Es esta herramienta la que se encarga de que los dos elementos propuestos (servidor web Apache y máquina virtual de Windows 10) estén funcionando sobre uno de los nodos del sistema, o incluso sobre varios a la vez para equilibrar la carga de trabajo. Además, si cae la máquina que está corriendo los servicios, se encarga de migrar a otra disponible según las preferencias que se hayan configurado.

En la **Figura 3.4.2** se observa que el servidor Apache y la máquina virtual están corriendo sobre el nodo *Raybian-HP*, en color verde, mientras que el clúster de datos está corriendo como primario en el nodo *Deb1*, en color amarillo. Se simula la situación en la que el nodo *Raybian-HP* cae y automáticamente los servicios pasan a funcionar desde el nodo *Raybian-msi*, en color azul, como se puede observar en la **Figura 3.4.3**.

²⁷ Fuente: Elaboración propia.

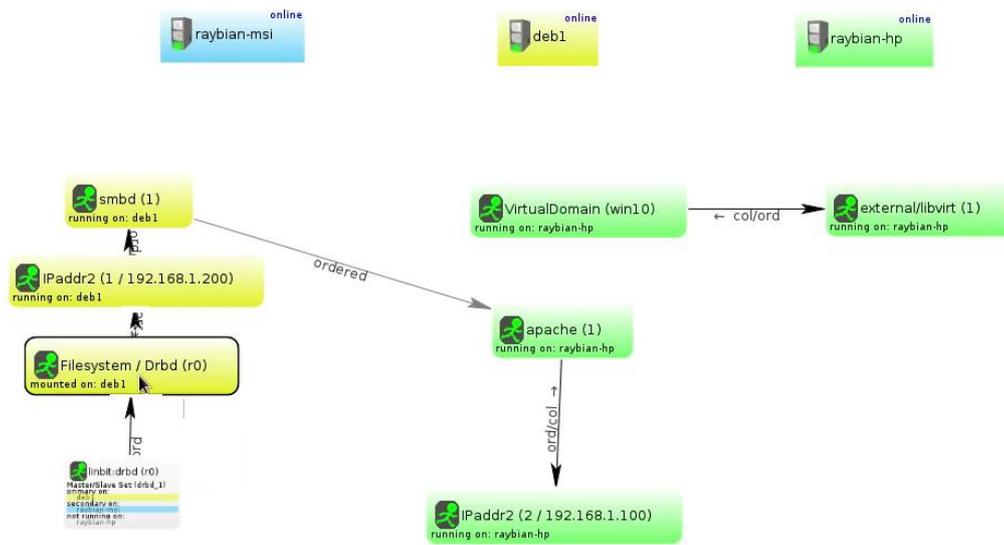


Figura 3.4.2 Servicios corriendo en nodo *Raybian-HP*.²⁸

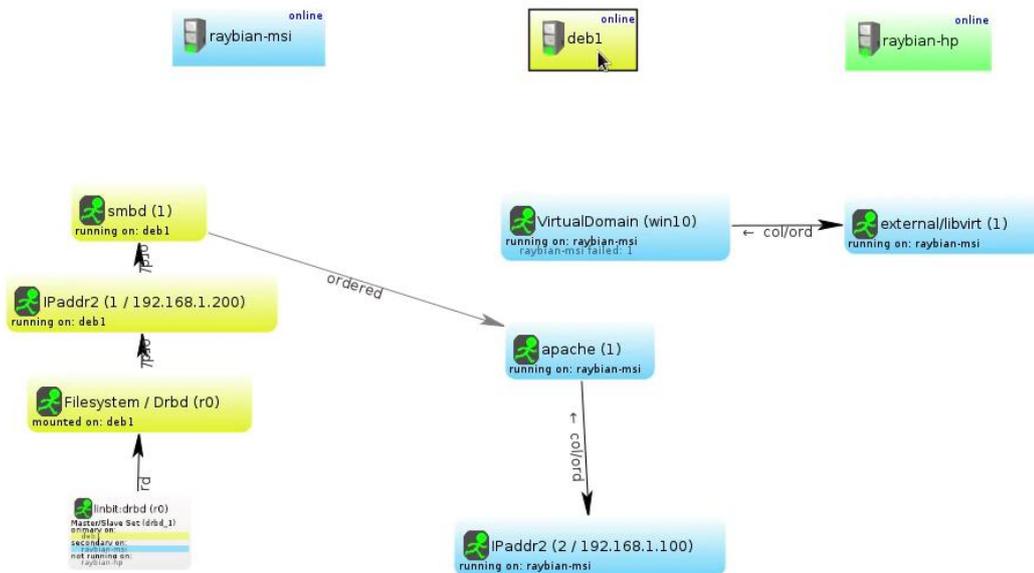


Figura 3.4.3 Servicios corriendo en nodo *Raybian-msi*.²⁹

Para ello, necesita las funciones de Corosync, que se encarga de la comunicación entre nodos y es quien avisa si alguno deja de estar en línea para que Pacemaker migre los servicios a otra máquina.

Si bien los datos pueden estar montados en forma de sistema de ficheros bien en *Raybian-msi* o bien en *deb1*, tanto KVM como Apache necesitan localizar sus recursos, win.qcow2 (archivo de disco de la máquina virtual de Windows 10) e index.html, de forma centralizada, para ello acceden a un repositorio creado con Samba y a través de

²⁸ Fuente: Elaboración propia.

²⁹ Fuente: Elaboración propia.

Práctica.

una dirección IP ,192.168.1.200 (representada por una nube en el gráfico), la cual es gestionada por Pacemaker. Esta dirección IP es vista como un recurso más para Pacemaker y se activa en la máquina adecuada en cada caso. Esto se hace para que, si en algún momento cae un equipo, siempre se pueda acceder a los datos a través de otro desde una misma dirección.

Para que esto sea posible, DRBD crea un clúster de datos que, junto al RAID 1, hace que la información redunde en varias localizaciones y con resistencia a errores de disco en la parte del RAID. En todo momento los dos discos del RAID se copian entre sí, y a la vez se respaldan en el tercer disco del clúster. Es, sin embargo, Pacemaker quien monta un sistema de ficheros *Ext4* en el Nodo marcado como principal, y Samba quien ofrece por red esos datos de forma localizada.

Para mantener la consistencia de estos datos y ante la caída o degradación de elementos del clúster se utilizan recursos Stonith, que en nuestro esquema evitan que varios nodos puedan corromper el clúster de datos. La situación anterior se da, por ejemplo, en casos en los que dos nodos quedan aislados entre ellos y se levantan ambos como primarios, accediendo a los datos del clúster sin control y corrompiéndolo. Stonith evita esta situación *cercando (fence)* al nodo degradado.

3.5 COMPARATIVA CON EL SISTEMA ACTUAL

Una vez finalizada la práctica, se va a proceder a la evaluación del sistema propuesto comparándolo con el que existe en la actualidad. Para ello se va a someter a una serie de variables, con valores entre 1 y 5, a una ponderación de acuerdo con la importancia de dichas variables, con valores entre 0 y 1.

Variables	Sist. Propuesto (KVM)	Sist. Actual (Win server 2012)	Ponderación
Facilidad de instalación	2	4	1
Facilidad de administración	5	4	0.8
Formación necesaria	2	4	1
Rendimiento	5	4	0.6
Seguridad	3	5	1
Portabilidad	4	2	0.5
Escalabilidad	5	3	0.5
Coste	5	2	0.8
Resultado	22.5	22.7	

Tabla 3.2 Evaluación comparativa del sistema actual VS sistema propuesto.³⁰

³⁰ Fuente: Elaboración propia.

Las ponderaciones más altas se han dado a las variables que se consideran más importantes a la hora de garantizar la seguridad y disponibilidad de la información. Por ello, las variables **seguridad** y **formación necesaria** son las que más ponderación han recibido. Esto es debido a que, con un personal no cualificado, no se puede garantizar la disponibilidad del sistema de información. La variable **facilidad de instalación**, también requiere una ponderación alta debido a que, está relacionada estrechamente con la variable **formación necesaria** y también puede mellar las capacidades del sistema, o incluso crear una posible brecha de seguridad.

Las variables **facilidad de administración, coste y rendimiento**, son las siguientes mejor valoradas. La primera, por el mismo motivo que las anteriores, la disponibilidad de la información. La variable **rendimiento** no es tan determinante como la variable **seguridad**, pero un rendimiento mayor mejoraría las capacidades del sistema, abriendo nuevas posibilidades en el futuro, pudiendo añadir nuevas aplicaciones o utilidades. Por último, la variable **coste** recibe una valoración alta por causas evidentes. Cualquier ahorro que no suponga una pérdida de capacidades siempre es positivo.

Las dos últimas variables, **portabilidad y escalabilidad**, reciben menos valoración ya que, el sistema no está diseñado con tales fines, pero pueden suponer ventajas para nuevas actualizaciones.

Conclusiones.

4 CONCLUSIONES

El sistema propuesto **cumple con los objetivos** marcados para este Trabajo de Fin de Grado ya que, utiliza las técnicas de virtualización, corre sobre software libre y es capaz de hacer funcionar servicios similares a los ofrecidos por SIMACET garantizando la alta disponibilidad de datos y procesos.

A la vista de los resultados de la **Tabla 3.2**, se observa que ambos sistemas obtienen puntuaciones muy similares. Sin embargo, hay tres parámetros que se deben tener muy en cuenta.

El primero es el parámetro de la seguridad, el cual, en ambos sistemas debería tener una puntuación de 5 para considerarse válido dada la importancia que tiene. No se puede poner en riesgo nunca la **seguridad de la información en el ámbito militar**, por ello, al no estar garantizada la seguridad del sistema ofrecido por el uso de SO Debian 9, se recomienda el uso de otros SO de software libre que, pagando la licencia correspondiente, pueden ofrecer más garantías.

El segundo, coste, es una variable que, evidentemente tiene un gran peso, pero no debe ser determinante a la hora de seleccionar un sistema de información para ambientes tácticos.

El tercer parámetro que hay que observar detenidamente es el de la formación necesaria. Esto se debe a que por muy bueno que sea un sistema, la **mayoría de los errores** que se dan suelen ser **humanos**. Por eso, disponer de un personal altamente cualificado requiere mucha formación, la cual, ha de administrar el Ejército de Tierra. Esto se traduce en costes en cursos de capacitación en entornos Linux que actualmente no se administran y que generarían costes adicionales.

Por experiencia propia, la creación y configuración del sistema hasta el correcto funcionamiento del mismo, tiene una **complejidad elevada** para usuarios que no estén familiarizados con el entorno Linux. Hacer funcionar un sistema de estas características pasa por un proceso complejo en el que, en este caso, ha requerido una gran parte del tiempo empleado en auto aprendizaje de todas las tecnologías utilizadas.

COMENTARIOS PERSONALES Y LÍNEAS FUTURAS DE TRABAJO

Teniendo en cuenta las conclusiones y los resultados obtenidos de las entrevistas con los administradores del Nodo SIMACET, considero que un sistema que reuniese las mejores condiciones haría uso de las tecnologías de virtualización y clúster de alta disponibilidad, como el propuesto. Sin embargo, debería correr sobre un SO Windows Server 2012 o pasar por una debida implementación realizada por los expertos en seguridad de la información para poder cumplir con las STIC de seguridad y que sea acreditable por la OTAN³¹.

³¹ OTAN: Organización del Tratado del Atlántico Norte.

Las STIC son normas emitidas por el CCN³² para cada sistema de información/tecnología en las que constan recomendaciones y configuraciones específicas de seguridad que deben llevarse a cabo escrupulosamente para que dichos sistemas sean acreditables desde el punto de vista de la seguridad de la información.

Para esta práctica se ha utilizado el SO Debian 9.1, un SO gratuito que no está garantizado por su proveedor. Sin embargo, como se ha mencionado anteriormente, existen otros SO de software libre de los cuales también se pueden pagar licencias y obtener una garantía que aumente las posibilidades de acreditación del sistema de la práctica por los expertos.

³² CCN: Centro Criptológico Nacional.

5 BIBLIOGRAFÍA

- [1] Defensa.com, «La innovación, clave en los sistemas de mando y control de Defensa», 2012. [En línea]. Disponible en: <http://www.defensa.com/analisis/innovacion-clave-sistemas-mando-control-defensa>. [Accedido: 02-nov-2017]
- [2] «Tutorial RAID: cómo elegir el nivel RAID adecuado». [En línea]. Disponible en: <http://searchdatacenter.techtarget.com/es/consejo/Tutorial-RAID-como-elegir-el-nivel-RAID-adecuado>. [Accedido: 31-oct-2017].
- [3] «Las ventajas de RAID (RAID 0 vs. RAID 1 vs. RAID 5)». [En línea]. Disponible en: <https://support.wdc.com/knowledgebase/answer.aspx?ID=3448&lang=ls>. [Accedido: 31-oct-2017].
- [4] «¿En qué consiste la configuración de discos duros en RAID?» [En línea]. Disponible en: <https://hipertextual.com/archivo/2014/01/que-es-raid-discos-duros/>. [Accedido: 31-oct-2017].
- [5] «Arreglos de discos (RAID) | Orlando Olgún Olvera». [En línea]. Disponible en: <https://orlandoolguin.wordpress.com/2010/06/21/arreglos-de-discos-raid/>. [Accedido: 31-oct-2017].
- [6] «Recuperar datos de un RAID 5 – Recuperando archivos perdidos». [En línea]. Disponible en: <http://recoverylostfiles.com/c-bfyd2je3y-3.php>. [Accedido: 31-oct-2017].
- [7] «Cluster de servidores, ¿qué es y como funciona?» [En línea]. Disponible en: <http://www.solingest.com/blog/cluster-de-servidores-que-es-y-como-funciona>. [Accedido: 31-oct-2017].
- [8] E. Villar y J. Gómez, «Introducción a La virtualización», 1996. [En línea]. Disponible en: <http://www.adminso.es>. [Accedido: 03-sep-2017].
- [9] «Máquinas virtuales: qué son, cómo funcionan y cómo utilizarlas». [En línea]. Disponible en: <https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas>. [Accedido: 31-oct-2017].
- [10] «Las ventajas y las desventajas de la virtualización de servidores». [En línea]. Disponible en: <http://rcg-comunicaciones.com/ventajas-e-inconvenientes-la-virtualizacion/>. [Accedido: 03-oct-2017].
- [11] «Ventajas y desventajas de la virtualización de servidores | JMG Virtual Consulting - Consultoría Tecnológica TIC». [En línea]. Disponible en: <https://www.jmgvirtualconsulting.com/2017/07/ventajas-y-desventajas-de-la-virtualizacion-de-servidores/>. [Accedido: 31-oct-2017].
- [12] «OpenStack - KVM vs Hyper-V - Scenario 1 - Cloudbase Solutions». [En línea]. Disponible en: <https://cloudbase.it/openstack-kvm-vs-hyper-v-part-2/>. [Accedido: 01-nov-2017].

- [13] «OpenStack Newton Benchmarking - Scenario 2 - Cloudbase Solutions». [En línea]. Disponible en: <https://cloudbase.it/openstack-newton-benchmarking-part-3/>. [Accedido: 01-nov-2017].
- [14] «OpenStack Newton Benchmarking - Scenario 3 (Hadoop) - Cloudbase Solutions». [En línea]. Disponible en: <https://cloudbase.it/openstack-newton-benchmarking-part-4-hadoop/>. [Accedido: 01-nov-2017].
- [15] «VIRTUALIZATION PERFORMANCE: VMWARE VSPHERE 5 VS. MICROSOFT HYPER---V R2 SP1 A PRINCIPLED TECHNOLOGIES TEST REPORT SUMMARY», 2011.
- [16] «Benchmark results of Random I/O performance of different RAID levels». [En línea]. Disponible en: <http://louwrentius.com/benchmark-results-of-random-io-performance-of-different-raid-levels.html>. [Accedido: 31-oct-2017].

6 ANEXOS

ANEXO A - ENTREVISTAS

Para poder conocer las deficiencias o debilidades del Nodo SIMACET se han realizado unas encuestas a los administradores del mismo, con el fin de poder ajustar el diseño del sistema y mejorar las capacidades.

Las encuestas se han centrado en conocer de primera mano las opiniones de los verdaderos usuarios administradores y expertos en este campo. Además, se les ha pedido una visión personal de las medidas que llevarían a cabo para poder solventar los problemas, debido a que, como administradores, son los mejores candidatos para obtener información fiable.

ENTREVISTA NÚMERO 1

SARGENTO ESPECIALISTA DON O.C.N.

¿Qué cambiaría usted en el Nodo SIMACET para poder mejorar su rendimiento y fiabilidad?

En primer lugar, renovaría todo el hardware de los servidores, ya que son máquinas, conectores y cableado muy antiguos, algunos obsoletos, y nos encontramos con problemas como falta de repuestos o repuestos muy difíciles de encontrar. Además del uso que se les ha dado, los conectores presentan ya muchas deficiencias que hacen que a veces el despliegue del Nodo se convierta en una tarea mucho más difícil de lo que debería. Un hardware más actual mejoraría también el rendimiento de los servicios que ofrecemos.

Por otro lado, el sistema tarda mucho en arrancar por completo. Esto es un problema especialmente cuando se cae por culpa de algún error crítico que obliga al reinicio de los servidores. El Mando no puede estar tanto tiempo sin el apoyo del Nodo.

Si se pudiera diseñar un sistema con una protección total ante errores ocasionales sin duda mejoraría la situación general del Nodo.

Ante estas situaciones ¿Cómo cree Ud. que se podría mejorar el sistema?

Como dije antes, con la compra de nuevos equipos se evitaría la primera situación.

Para las demás situaciones considero que un gran paso sería virtualizar el sistema. Con ello si cae un servicio no afectaría al resto y el impacto sería menor, lo que aumenta la resistencia del sistema ante errores. Además, si cae un servidor principal el otro podría mantener funcionando los servicios hasta que se recupere el primero, sin que el Mando sepa que algo ha fallado.

Anexos.

ENTREVISTA NÚMERO 2

SARGENTO ESPECIALISTA DON C.R.E.

¿Qué cambiaría usted en el Nodo SIMACET para poder mejorar su rendimiento y fiabilidad?

Un gran problema que creo que afecta al Nodo es el de la temperatura que se genera en su interior. Es un espacio muy reducido que alberga muchas máquinas en su interior y se genera mucho calor, esto para los propios servidores crea un efecto muy negativo.

Además, cuando arrancan los servidores pasa demasiado tiempo hasta que los servicios son accesibles para el Jefe del Puesto de Mando al que apoyamos. Lo que implica que si necesitamos reiniciar el equipo tardamos demasiado tiempo en volver a dar servicio.

Ante estas situaciones ¿Cómo cree Ud. que se podría mejorar el sistema?

Una reestructuración física del interior del Nodo consiguiendo algo más de espacio, o algún sistema que favorezca una mayor ventilación podrían mejorar el problema de la temperatura que se genera.

Los equipos de los que disponemos son muy antiguos pero suficientes para el servicio que debemos dar, sin embargo, con equipos más modernos reduciríamos los tiempos de carga del sistema mejorando el servicio que debemos ofrecer.

ENTREVISTA NÚMERO 3

SARGENTO ESPECIALISTA DON F.P.M.

¿Qué cambiaría usted en el Nodo SIMACET para poder mejorar su rendimiento y fiabilidad?

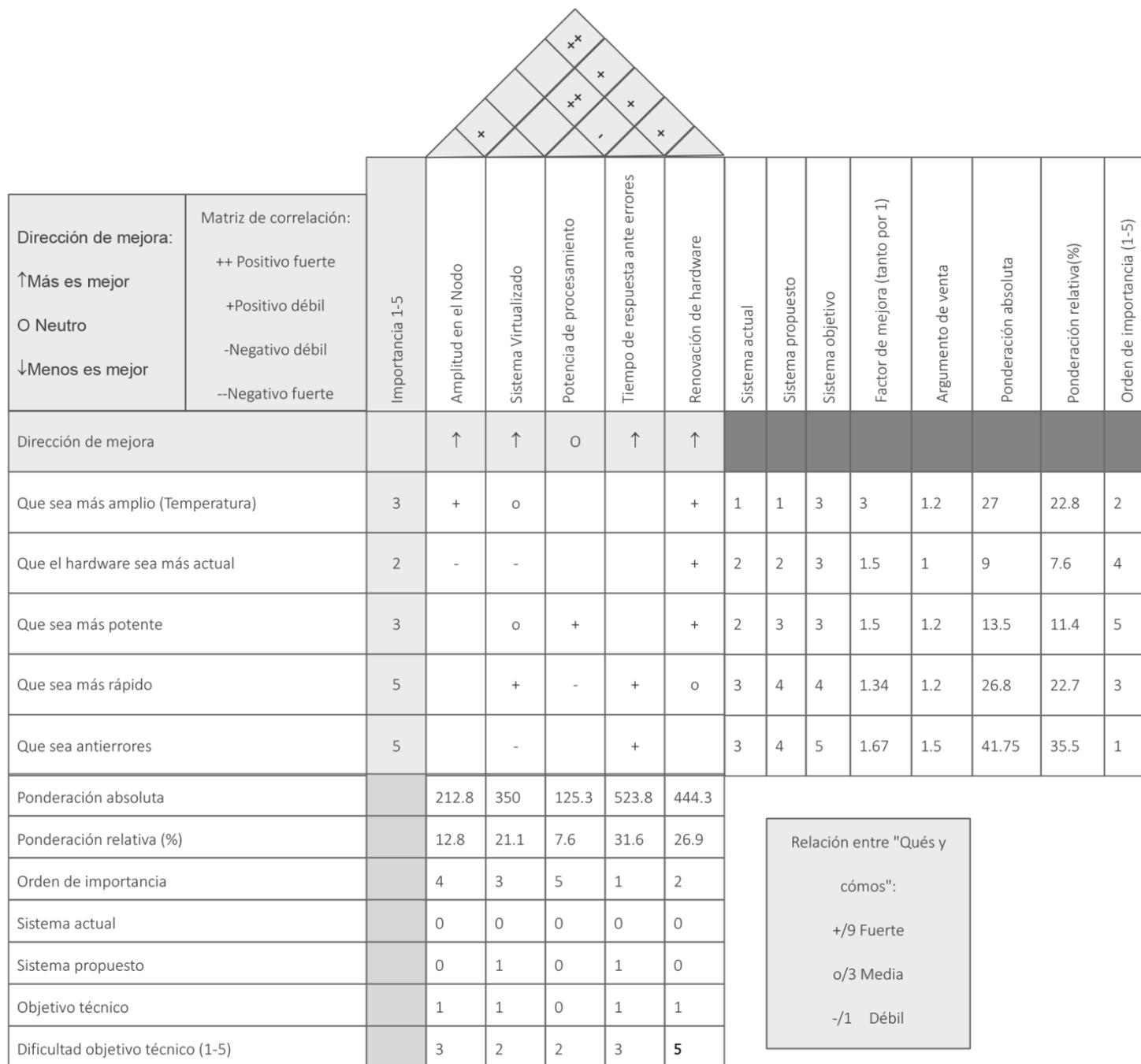
Considero que un sistema que ofrece tantos servicios, y con una importancia como la que tiene SIMACET dentro de la maniobra, debería ser más potente y más fiable. Que disponga de una buena protección frente a errores fatales que hagan caer al servidor.

Además, a veces puede llegar a resultar muy lento. Lo que puede hacer que deje de cumplir la misión principal del sistema, que es ofrecer una fuente de información fiable a tiempo casi real.

Ante estas situaciones ¿Cómo cree Ud. que se podría mejorar el sistema?

No considero que cambiar los servidores sea de máxima prioridad, pero sí cambiaría la configuración del sistema, por ejemplo, utilizando un clúster de alto rendimiento, que aumentaría las capacidades del sistema.

Otra posibilidad sería configurarlo creando un clúster de alta disponibilidad, lo cual nos ofrece un escudo anti errores. Para que el sistema se viniese abajo tendrían que caer todos los servidores, y es algo que normalmente no ocurre.

ANEXO B – FUNCIÓN QFD

Figura B.1 Función QFD.³³

A raíz de las entrevistas realizadas a los administradores del Nodo SIMACET se han extraído los puntos a mejorar del mismo, y posibles soluciones para poder mejorarlo.

³³ Fuente: Elaboración propia.

Anexos.

Éstas se han utilizado para realizar una función QFD³⁴ para saber cuál es la ponderación que dan los operadores a las posibles mejoras del sistema. Así, la persona o equipo encargados de una actualización del mismo pueden saber qué aspectos son más importantes o en cuales centrarse con más dedicación.

Para cuantificar los “Cómos” de la función QFD se ha utilizado los valores 1 y 0 para determinar si las características propuestas están presentes o no, tanto en el sistema actual como en el propuesto.

En este caso se han extraído varios puntos que pueden ser mejorables, tales como la temperatura generada en el interior del Nodo o la resistencia ante errores del sistema. Algunas soluciones propuestas son interesantes, aunque no son objeto de este proyecto, como la adquisición de nuevos equipos o la reestructuración de la distribución física del shelter³⁵ que lo contiene. Sin embargo, existen otras que sí están al alcance del diseño del nuevo sistema, como el uso de la tecnología de virtualización o la configuración en clúster de los servidores en las modalidades de alto rendimiento o alta disponibilidad.

Los resultados de la función determinan que para los usuarios la primera prioridad reside en mejorar el tiempo de respuesta ante los errores, seguido de la virtualización del sistema y por último aumentar la potencia de procesamiento. Las otras dos mejoras propuestas se han obviado en el resultado de la función debido a que no son objeto del estudio de este proyecto.

³⁴ Quality Function Deployment o “despliegue de la casa de la calidad”

³⁵ Contenedor acoplable a los camiones del Ejército de Tierra

ANEXO C – COMPARATIVA DE HIPERVISORES KVM VS HYPER-V VS VMWARE

Para saber si el sistema diseñado estará a la altura de las dos alternativas que actualmente se usan en el entorno del Ejército de Tierra se realizará una comparativa de rendimiento, ya que en cuanto al apartado económico KVM no tiene rival.

Para ello se van a observar gráficas de rendimiento de diferentes pruebas a las que han sido sometidos los diferentes hipervisores, encontradas en diversas páginas web y blogs de virtualización, tales como cargar máquinas virtuales, eliminarlas, o activar otros servicios diferentes.

C.1 PRUEBAS KVM VS HYPER-V

Para la primera prueba de rendimiento se va a solicitar a ambos hipervisores a cargar una máquina virtual, esperar a que esté activa y por último borrarla.[12]

Results for **KVM** running on **Xenial Ubuntu 16.04.1 LTS** (default kernel version 4.4.0-45-generic):

Load duration: **171.627 s** Full duration: **177.795 s** Iterations: **200** Failures: **0**

Total durations

Action	Min (sec)	Median (sec)	90%ile (sec)	95%ile (sec)	Max (sec)	Avg (sec)	Success	Count
nova.boot_server	8.444	35.426	39.162	41.148	45.956	33.584	100.0%	200
nova.delete_server	2.508	5.071	5.791	6.98	7.645	5.044	100.0%	200
total	12.485	39.535	42.46	45.356	50.389	37.627	100.0%	200

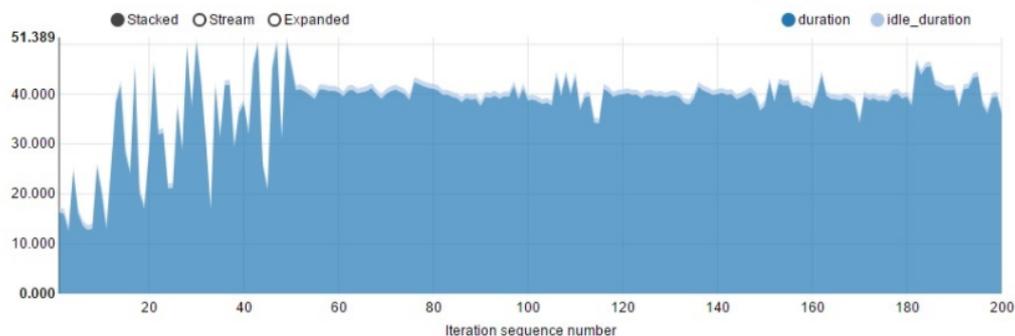


Figura C.1.1 Resultado de la primera prueba de KVM.³⁶

³⁶ Fuente: <https://cloudbase.it/>

Anexos.

Results for **Hyper-V / Windows Server 2012 R2**:

Load duration: **207.795 s** Full duration: **213.757 s** Iterations: **200** Failures: **0**

Total durations

Action	Min (sec)	Median (sec)	90%ile (sec)	95%ile (sec)	Max (sec)	Avg (sec)	Success	Count
nova.boot_server	6.971	44.085	45.836	47.712	206.297	43.44	100.0%	200
nova.delete_server	2.479	2.677	2.945	3.048	3.273	2.723	100.0%	200
total	8.532	45.823	47.527	49.491	207.776	45.163	100.0%	200

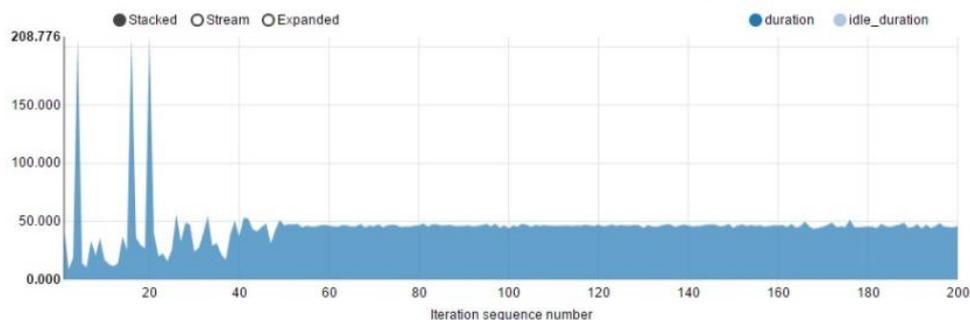


Figura C.1.2 Resultado de la primera prueba de Hyper-V.³⁷

En la primera prueba realizada se puede comprobar que KVM ofrece un tiempo medio de respuesta de casi ocho segundos menos que Hyper-V.

Para la segunda prueba se añadirán dos acciones más a las anteriores, crear una IP flotante y una conexión SSH.[13]

Results for **KVM with Xenial Ubuntu 16.04.1 LTS** (default kernel version 4.4.0-45-generic) as host operating system:

Load duration: **341.586 s** Full duration: **383.616 s** Iterations: **200** Failures: **0**

Total durations

Action	Min (sec)	Median (sec)	90%ile (sec)	95%ile (sec)	Max (sec)	Avg (sec)	Success	Count
vm.wait_for_ssh	30.147	36.102	37.527	38.001	39.167	35.733	100.0%	200
vm.attach_floating_ip	2.901	4.87	6.342	6.875	7.733	5.032	100.0%	200
vm.delete_floating_ip	2.482	4.257	5.464	5.823	6.684	4.241	100.0%	200
nova.boot_server	9.424	21.468	45.496	57.108	68.991	25.899	100.0%	200
nova.delete_server	2.682	5.878	8.682	10.456	13.675	6.488	100.0%	200
total	59.352	71.652	102.73	111.839	121.703	76.469	100.0%	200

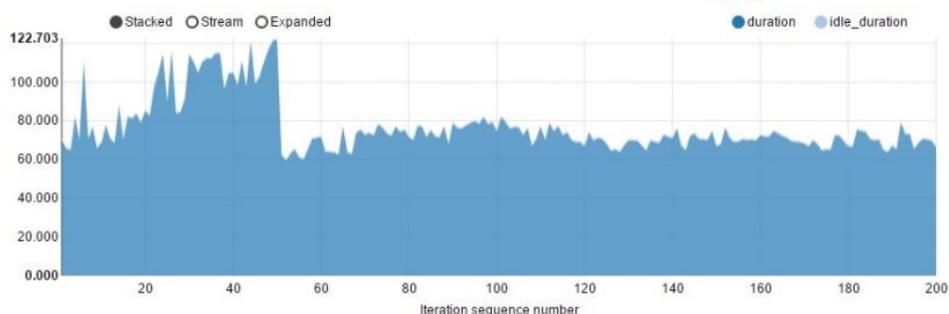


Figura C.1.3 Resultado de la segunda prueba de KVM.³⁸

³⁷ Fuente: <https://cloudbase.it/>

³⁸ Fuente: <https://cloudbase.it/>

Results for **Hyper-V** with **Windows Server 2012 R2** as host operating system:

Load duration: **250.523 s** Full duration: **293.219 s** Iterations: **200** Failures: **0**

Total durations

Action	Min (sec)	Median (sec)	90%ile (sec)	95%ile (sec)	Max (sec)	Avg (sec)	Success	Count
vm.wait_for_ssh	11.94	15.799	18.134	18.824	20.129	15.758	100.0%	200
vm.attach_floating_ip	3.058	7.619	8.883	9.314	10.921	7.359	100.0%	200
vm.delete_floating_ip	2.523	7.481	8.884	9.31	11.723	6.956	100.0%	200
nova.boot_server	13.286	18.511	42.649	53.226	64.714	23.15	100.0%	200
nova.delete_server	2.68	3.89	4.468	4.639	6.574	3.832	100.0%	200
total	41.736	52.183	77.701	88.84	98.707	56.132	100.0%	200

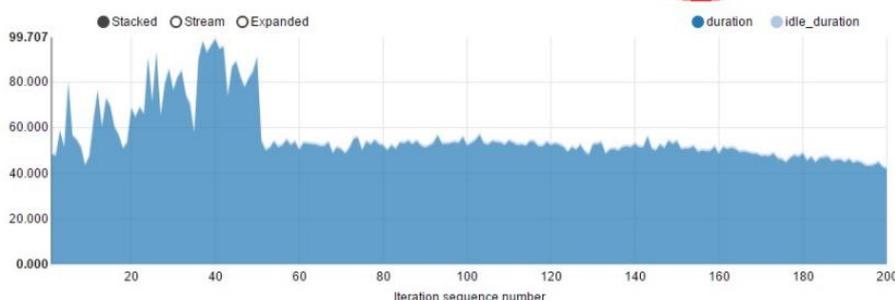


Figura C.1.4 Resultado de la segunda prueba de Hyper-V.³⁹

En este caso, el claro vencedor ha sido Hyper-V con casi veinte segundos menos en realizar todas las operaciones. La operación culpable de ello ha sido la de crear la conexión SSH con la máquina virtual, en el resto de pruebas se ha mostrado un rendimiento muy similar.

Para la tercera prueba se somete a los hipervisores a varias acciones con una peculiaridad, que deben hacerlas con diez máquinas virtuales corriendo a la vez en paralelo.[14]

³⁹ Fuente: <https://cloudbase.it/>

Anexos.

Results for **KVM** with **Xenial Ubuntu 16.04.1 LTS** (default kernel version 4.4.0-45-generic) as host operating system:

Load duration: **224.086 s** Full duration: **239.219 s** Iterations: **10** Failures: **0**

Total durations

Action	Min (sec)	Median (sec)	90%ile (sec)	95%ile (sec)	Max (sec)	Avg (sec)	Success	Count
vm_wait_for_ping	6.028	6.035	7.03	7.03	7.03	6.346	100.0%	10
vm_job_TeraGen	18.429	30.42	38.011	38.065	38.119	28.821	100.0%	10
vm_job_TeraSort	123.347	127.133	131.592	132.072	132.552	127.568	100.0%	10
nova.boot_server	11.582	13.488	15.016	15.243	15.469	13.431	100.0%	10
nova.delete_server	2.735	4.917	5.256	5.263	5.27	4.37	100.0%	10
vm.wait_for_ssh	12.358	13.394	14.375	14.387	14.398	13.301	100.0%	10
vm_job_TeraValidate	9.524	15.607	29.566	30.796	32.025	19.027	100.0%	10
vm.attach_floating_ip	2.59	2.964	3.372	3.486	3.6	2.998	100.0%	10
vm.delete_floating_ip	2.336	2.714	3.125	3.206	3.288	2.775	100.0%	10
total	218.017	222.002	222.961	223.522	224.083	221.638	100.0%	10

Figura C.1.5 Resultado de la tercera prueba de KVM.⁴⁰

Results for **Hyper-V** with **Windows Server 2012 R2** as host operating system:

Load duration: **234.524 s** Full duration: **249.361 s** Iterations: **10** Failures: **0**

Total durations

Action	Min (sec)	Median (sec)	90%ile (sec)	95%ile (sec)	Max (sec)	Avg (sec)	Success	Count
vm_wait_for_ping	8.031	9.534	10.05	10.054	10.057	9.141	100.0%	10
vm_job_TeraGen	20.723	23.453	50.861	51.084	51.307	31.076	100.0%	10
vm_job_TeraSort	96.163	134.232	139.898	143.075	146.253	127.766	100.0%	10
nova.boot_server	7.408	12.344	15.423	16.135	16.847	12.205	100.0%	10
nova.delete_server	2.551	2.735	4.871	4.892	4.914	3.322	100.0%	10
vm.wait_for_ssh	12.701	13.529	14.443	14.902	15.36	13.819	100.0%	10
vm_job_TeraValidate	7.442	9.984	14.113	14.935	15.757	10.928	100.0%	10
vm.attach_floating_ip	2.44	2.664	2.792	2.944	3.096	2.662	100.0%	10
vm.delete_floating_ip	2.051	2.197	2.732	2.742	2.751	2.349	100.0%	10
total	177.685	222.224	226.384	230.452	234.52	219.237	100.0%	10

Figura C.1.6 Resultado de la tercera prueba de Hyper-V.⁴¹

El resultado ofrecido en esta tercera y última prueba es casi idéntico, con una diferencia de tan solo dos segundos. Además, es el entorno más parecido al que se encontrarían ambos hipervisores en el Nodo SIMACET al correr todos los servicios bajo máquinas virtuales en paralelo. Para la realización de estas pruebas de rendimiento, el autor ha utilizado la herramienta Openstack.

La conclusión de estas tres pruebas es que los rendimientos de Hyper-V y KVM son muy similares con pequeñas diferencias perfectamente asumibles para el sistema propuesto.

C.2 PRUEBAS HYPER-V VS VMWARE

Es el turno de la comparativa de rendimiento entre las dos alternativas de pago, para ello se somete a los dos hipervisores a una prueba en la que corren a la vez treinta

⁴⁰ Fuente: <https://cloudbase.it/>

⁴¹ Fuente: <https://cloudbase.it/>

máquinas virtuales y se miden las órdenes por minuto que son capaces de realizar. [15]

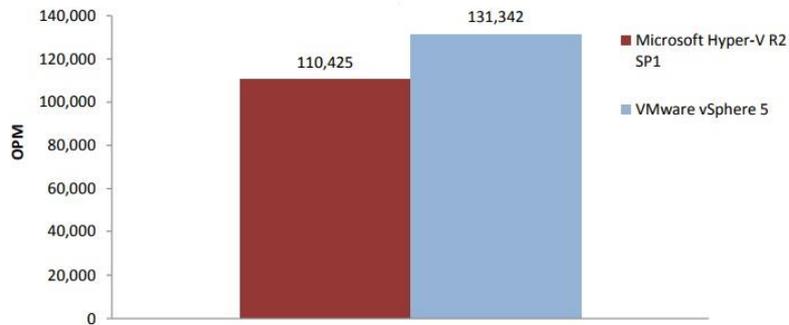


Figura C.2.1 Resultado de la primera prueba de Hyper-V VS vSphere.⁴²

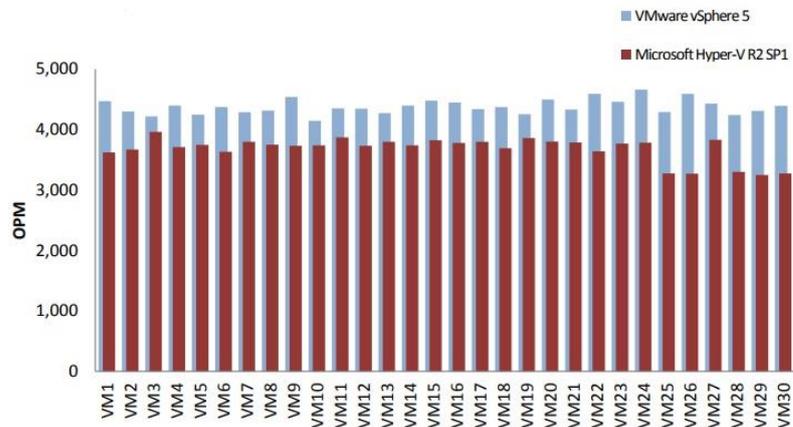


Figura C.2.2 Resultado de la segunda prueba de Hyper-V VS vSphere.⁴³

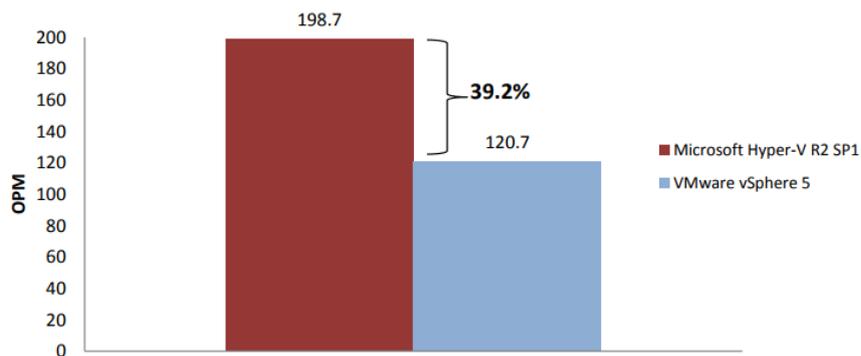


Figura C.2.3 Resultado de la tercera prueba de Hyper-V VS vSphere.⁴⁴

⁴²Fuente: <https://www.vmware.com>

⁴³Fuente: <https://www.vmware.com>

⁴⁴Fuente: <https://www.vmware.com>

Anexos.

La tercera prueba muestra una mayor desviación estándar del rendimiento de las máquinas virtuales cuando corren sobre Hyper-V. Una desviación menor muestra que las máquinas están corriendo con un rango de rendimiento menor, mostrando todas un comportamiento similar y más predecible.

A raíz de las tres pruebas se puede comprobar que el rendimiento de vSphere es algo superior respecto al de Hyper-V. Sin embargo, ambos hipervisores ofrecen una serie de características similares, por lo que, el rendimiento no es un factor determinante para esta práctica.

ANEXO D – PRUEBAS DE RENDIMIENTO RAID

Para la elección de un sistema de almacenamiento adecuado para la práctica se han consultado pruebas de rendimiento de los diferentes tipos de almacenamiento RAID existentes. Para ello se ha sometido a cada tipo a las mismas pruebas obteniendo una serie de gráficos que muestran el comportamiento de los mismos.[16]

El hardware utilizado para la realización de las pruebas es el siguiente:

- ✓ CPU: Intel Core i5 2400s @ 2.5 GHz.
- ✓ RAM: 4 GB.
- ✓ Discos: 6 x 500 GB, 7200 RPM drives (SATA).
- ✓ SO: Ubuntu Linux.
- ✓ RAID: Build-in Linux software RAID (MDADM).
- ✓ Tamaño de los archivos de prueba: 10 GB.

Los niveles RAID testeados han sido:

- ✓ RAID 0.
- ✓ RAID 10.
- ✓ RAID 5.
- ✓ RAID 6.

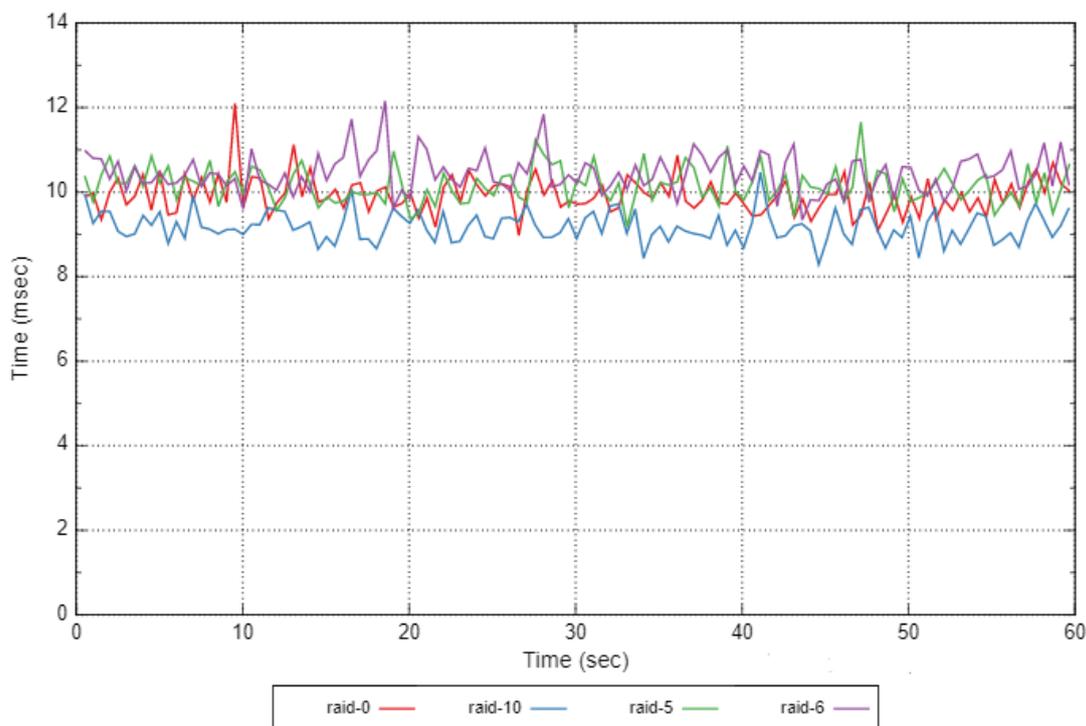


Figura D.1 Tiempo de respuesta.⁴⁵

⁴⁵ Fuente: <http://louwrentius.com>

Anexos.

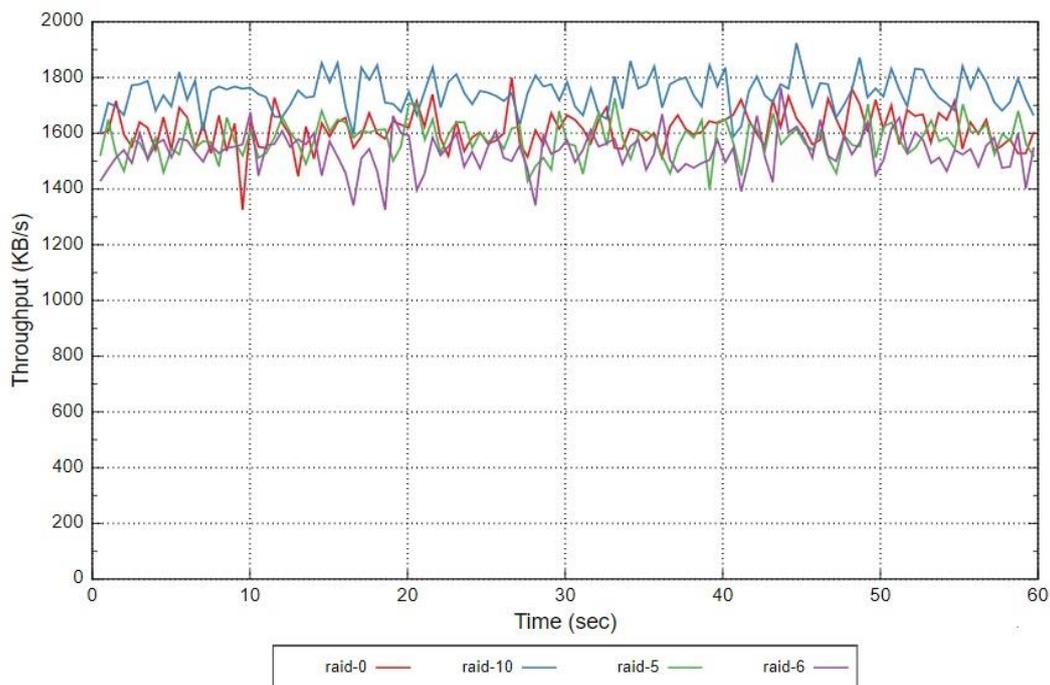


Figura D.2 Rendimiento de lectura de archivos.⁴⁶

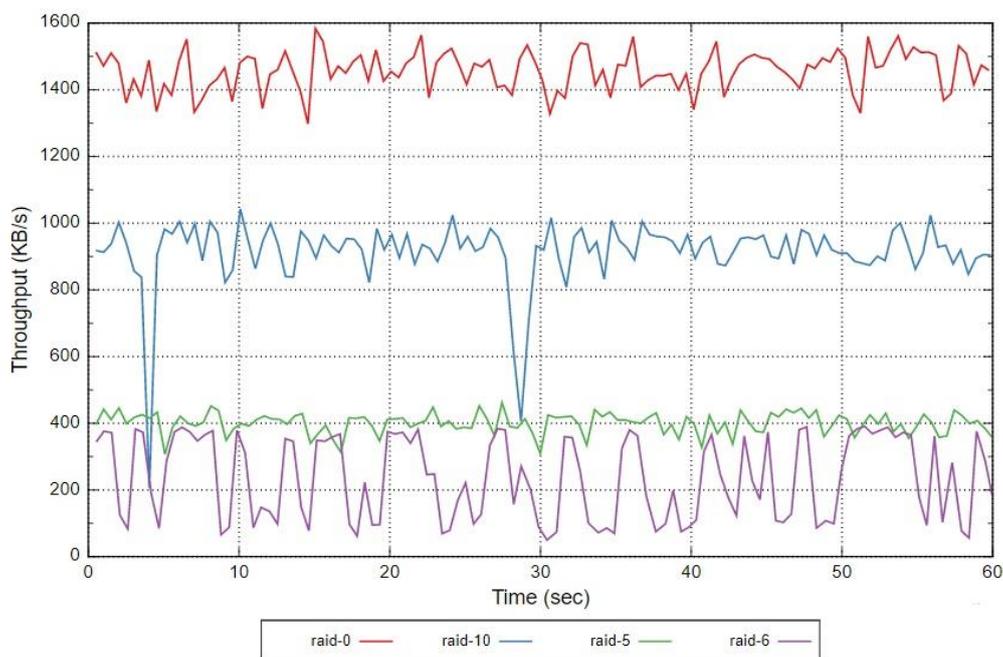


Figura D.3 Rendimiento de escritura de archivos.⁴⁷

En casi todas las situaciones el RAID 10 ofrece muy buenos resultados o incluso los mejores, ofreciendo el menor tiempo de respuesta ante operaciones, la mayor velocidad en cuanto a lectura, y un segundo puesto frente al RAID 0 en cuanto a escritura de archivos. No hay que olvidar que este sistema aglutina las ventajas del

⁴⁶ Fuente: <http://louwrentius.com>

⁴⁷ Fuente: <http://louwrentius.com>

RAID 1 y el RAID 0, combinando la velocidad de lectura/escritura, con la alta disponibilidad de los datos.

Por ello este sistema de almacenamiento es el idóneo para el diseño de la práctica del montaje de los servidores, teniendo en cuenta que carece de la recuperación de archivos en caso de corrupción de las unidades de disco. En este caso esa característica no es necesaria debido a que los datos solo deben ser accesibles para los ejercicios o maniobras ya que después resultan inútiles.