



Virtualització de Infraestructura de codi obert

César Reyes Rodríguez

Grau de Tecnologies de Telecomunicació, especialitat Telemàtica
Administració de Xarxes i Sistemes Operatius

Juan Ramon Esteban Grifoll

Javier Panadero Martínez

06/2019



Aquesta obra està subjecta a una llicència de [Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

FITXA DEL TREBALL FINAL

Títol del treball:	<i>Virtualització de Infraestructura de codi obert</i>
Nom de l'autor:	<i>César Reyes Rodríguez</i>
Nom del consultor/a:	<i>Juan Ramon Esteban Grifoll</i>
Nom del PRA:	<i>Javier Panadero Martínez</i>
Data de lliurament (mm/aaaa):	<i>06/2019</i>
Titulació o programa:	<i>Grau de Tecnologies de Telecomunicació, especialitat Telemàtica</i>
Àrea del Treball Final:	<i>Administració de Xarxes i Sistemes Operatius</i>
Idioma del treball:	<i>Català.</i>
Paraules clau	<i>Hipervisor, Commutador, Virtual</i>
Resum del Treball (màxim 250 paraules): <i>Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball</i>	
<p>La virtualització de la infraestructura mitjançant codi obert permet oferir els mateixos recursos que qualsevol infraestructura física amb certs avantatges. Amb la virtualització s'aprofita al màxim la capacitat dels servidors, es redueix el temps d'inactivitat i s'estalvia una gran quantitat d'energia. Amb el programari lliure disminueixen els cost d'adquisició de llicències, es requereix maquinari amb menor capacitat i augmenta la durabilitat de les solucions.</p> <p>En aquest treball es pretén donar una solució a l'obsolescència del maquinari informàtic a baix cost mitjançant la virtualització. S'exposa el punt de partida, les anàlisis i les justificacions que porten a definir una combinació de diferents tecnologies de virtualització que permetran oferir una solució a l'inconvenient de treballar amb maquinari obsolet.</p> <p>Per a realitzar aquesta solució, s'han repassat i estudiat diferents tecnologies que han portat a definir KVM com Hipervisor i Open vSwitch com a commutador virtual per a crear qualsevol escenari capaç d'implementar-se com a centre neuràlgic de la infraestructura amb totals garanties en el seu funcionament.</p>	

Abstract (in English, 250 words or less):

The virtualization of the infrastructure through open source allows to offer the same resources as any physical infrastructure with certain advantages. With virtualization, server capacity is maximized, downtime is reduced and a large amount of energy is saved. With free software, the cost of acquiring licenses decreases, hardware with less training is required and the durability of the solutions increases.

In this work, it is intended to provide a solution to obsolescence at low cost through virtualization. It exposes the starting point, the analyzes and the justifications that lead to define a combination of different virtualization technologies that will offer a solution to the inconvenience of working with obsolete hardware.

To carry out this solution, different technologies have been reviewed and studied that have led to define KVM as Hypervisor and Open vSwitch as a virtual switch to create any scenario that can be implemented as the nerve center of the infrastructure with full guarantee in its operation.

Agraïments

A la família.

A totes la persones que m'han animat a realitzar el grau.

A totes les persones que m'han ajudat d'una forma o una altra en els meus estudis.

Índex

1	INTRODUCCIÓ	4
1.1	CONTEXT I JUSTIFICACIÓ DEL TREBALL	4
1.2	OBJECTIUS DEL TREBALL	5
1.3	ENFOCAMENT I MÈTODE SEGUIT	5
1.4	PLANIFICACIÓ DEL TREBALL	6
1.5	BREU DESCRIPCIÓ DELS ALTRES CAPÍTOLS DE LA MEMÒRIA	7
2	TECNOLOGIES DE VIRTUALITZACIÓ DE MAQUINARI	9
2.1	REPÀS A LA HISTÒRIA DE LA VIRTUALITZACIÓ.	9
2.2	CARACTERÍSTIQUES DE LA VIRTUALITZACIÓ	9
2.3	PROS I CONTRES ACTUALS EN LA TECNOLOGIA DE LA VIRTUALITZACIÓ.....	10
2.4	HIPERVISOR	11
2.4.1	HIPERVISOR NATIU O TIPUS 1	11
2.4.2	HIPERVISOR ALLOTJAT O TIPUS 2	12
2.4.3	HÍBRIDS	13
2.5	TECNOLOGIES DERIVADES	14
2.5.1	VIRTUALITZACIÓ EN CONTENIDORS.....	14
2.5.2	CLOUD COMPUTING.....	14
3	TECNOLOGIES DE VIRTUALITZACIÓ DE XARXA	15
3.1	HIPERVISOR DE XARXA.....	15
3.2	COMMUTADOR VIRTUAL	16
3.3	XARXA SUPERPOSADA, OVERLAY NETWORK	16
3.4	OPENSTACK	17
3.5	XARXES MULTI TENANT	18
3.6	VIRTUALITZACIÓ DE LES FUNCIONS DE XARXA	18
4	PUNT DE PARTIDA	19
5	ANÀLISIS	22
5.1	PROBLEMES DERIVATS DE LA UTILITZACIÓ DE INFRAESTRUCTURA OBSOLETA	22
5.2	POSSIBLES SOLUCIONS	23
5.2.1	SOLUCIÓ MITJANÇANT UNA POLÍTICA DE CONTINUÏTAT	24
5.2.2	SOLUCIÓ MITJANÇANT LA VIRTUALITZACIÓ.....	25
5.3	JUSTIFICACIÓ DE LA SOLUCIÓ TRIADA	27
6	MODEL	28

7	JUSTIFICACIONS	30
7.1	PROGRAMARI LLIURE	30
7.2	ELECCIÓ DEL HIPERVISOR.....	32
7.2.1	PRINCIPALS PROVEÏDORS DE SOFTWARE DE VIRTUALIZACIÓ	32
7.2.2	VIRTUAL BOX	33
7.2.3	XEN.....	34
7.2.4	KVM.....	34
7.2.5	CONCLUSIONS	36
7.3	SISTEMA OPERATIU PER ALLOTJAR L’HIPERVISOR.....	37
7.4	MAQUINARI VIRTUALITZAT	38
7.4.1	TALLAFOCs	38
7.4.2	SERVIDOR DE DOMINI.....	39
7.4.3	SERVIDOR WEB Y SERVIDOR FTP.....	41
7.5	SERVIDOR DE VITALITZACIÓ.	42
7.6	NAS, NETWORK ATTACHED STORAGE	43
7.7	XARXA VIRTUAL PER L’HIPERVISOR.	43
7.7.1	NETWORK SERVICE	44
7.7.2	SUITE ‘IPROUTE2’.....	44
7.7.3	OPEN VIRTUAL SWITCH	46
8	IMPLEMENTACIÓ	51
8.1	INSTAL·LACIÓ DEL SISTEMA OPERATIU	51
8.2	INSTAL·LACIÓ DE KVM	51
8.3	INSTAL·LACIÓ DE OPEN VSWITCH	52
8.4	PREPARACIÓ DE LES XARXES VIRTUALS	53
8.5	CREACIÓ DE LES MÀQUINES VIRTUALS	57
9	VALORACIÓ ECONÒMICA	60
10	CONCLUSIONS.....	63
11	GLOSSARI.....	65
12	BIBLIOGRAFIA	67
13	ANNEXOS.....	68
13.1	ARXIU DE CONFIGURACIÓ DE LES INTERFÍCIES VIRTUALS.....	68
13.2	ARXIU DE CONFIGURACIÓ DE LES INTERFÍCIES FÍSQUES.....	69
13.3	ESPECIFICACIONS, DELL POWER EDGE R340 ENRACKABLE	70
13.4	ESPECIFICACIONS, SYNOLOGY NAS	71

Llista de figures

Figura 1. Tasques del TFG.....	7
Figura 2. Diagrama de Gantt del TFG	7
Figura 3. Hipervisor tipus 1 o natiu.....	12
Figura 4. Hipervisor tipus 2 o allotjat	13
Figura 5. Arquitectura SDN.	15
Figura 6. Commutadors virtuals	16
Figura 7. Estructura Overlay Network	17
Figura 8. Open Stack, Virtual + Física.....	17
Figura 9. Esquema lògic, Xarxa Multi Tenant.....	18
Figura 10. Infraestructura actual.....	20
Figura 11. Esquema lògic de la de la proposta	23
Figura 12. Esquema del model.....	28
Figura 13. Valoracions de Hipervisors.....	32
Figura 14. pfSense	39
Figura 15. Zentyal Server	40
Figura 16. Configuració servidors DMZ.....	41
Figura 17. Bridge.....	45
Figura 18. Vlan	45
Figura 19. Macvtap.....	45
Figura 20. Procés d'intercanvi de OVS.....	47
Figura 21. Principal components de OVS	48
Figura 22. Screenshot Instal·lació de CentOS7	51

Llista de taules

Taula 1. Requisits mínims de memòria per al Servidor de Virtualització	42
Taula 2. Desglossament i cost de material, Infraestructura física de Xarxa	60
Taula 3. Desglossament i cost del Material, Sistemes	60
Taula 4. Cost total del Material.....	61
Taula 5. Desglossament i cost de tasques, Tècnic especialista.....	61
Taula 6. Desglossament i cost de tasques, Administrador de Sistemes	61
Taula 7. Desglossament i cost de tasques, Tècnic de Sistemes.....	62
Taula 8. Cost total del Personal	62
Taula 9. Cost total del projecte	62

1 Introducció

1.1 Context i justificació del Treball

L'obsolescència programada garanteix que els consumidors comprin els productes en múltiples ocasions en lloc d'una sola vegada. Naturalment, això incrementa la demanda de productes perquè els consumidors han de continuar consumint una vegada i una altra. Un usuari ha de adquirir més vegades el mateix producte que si aquest producte fos resistent i li durés tota la vida.

Els sistemes operatius de Linux són més lleugers, eficaços i funcionals que els sistemes propietaris més coneguts, encara que es pot afirmar que les seves últimes versions són molt més pesades i algunes compten amb una interfície molt més sofisticada. A l'hora d'executar processos, les distribucions Linux consumeixen molts menys recursos, executen menys processos i funcionen de manera més ràpida i àgil.

Mitjançant la virtualització es poden executar diversos sistemes operatius i múltiples aplicacions alhora utilitzant un sol equip físic. Moltes organitzacions s'estan desfent de gran quantia de maquinari i estan integrant tots els serveis en màquines capaços d'allotjar els diferents sistemes, ja que els servidors de virtualització aprofiten de forma més eficaç els recursos materials disponibles.

A través d'aquest treball es vol aportar una solució a l'obsolescència programada dels equips informàtics, aportar una solució per ampliar la durabilitat dels recursos informàtics. A més, es vol relacionar la utilització de dos recursos tecnològics que per ells mateixos fan possible que els equips durin més temps. Es vol fer entendre que amb la combinació de la virtualització de maquinari i la utilització de programari lliure pot disminuir significativament els recursos necessaris i augmentar la durabilitat dels mateixos.

La virtualització permet gestionar el centre de treball com una agrupació de tota la capacitat de processament, memòria, xarxa i emmagatzematge disponible en la nostra infraestructura. Cada màquina virtual està aïllada de la resta, en cas d'ocórrer un bloqueig o una fallada general de sistema d'una de les màquines virtuals, no afectarà als altres elements.

Amb la virtualització els processos de la infraestructura són més ràpids i eficients, els mitjans d'emmagatzematge, com discs durs i unitats de cinta poden ser fàcilment afegits, i l'espai d'emmagatzematge també es pot compartir entre els diferents servidors. De la mateixa manera, la virtualització permet reforçar múltiples recursos i proporciona una oportunitat per consolidar l'arquitectura de sistemes, base de dades, interfícies, xarxes, escriptoris, i fins i tot processos de negocis, resultant en estalvis de costos i major eficiència.

1.2 Objectius del Treball

Aquest treball girarà al voltant de un cas d'us on es necessita implementar infraestructures virtualitzades a baix cost.

Els objectius principals d'aquest treball son els següents:

- Identificar els passos per l'aplicació d'una idea en un projecte real.
- Trobar una solució de confiança per contrarestar la obsolescència del maquinari
- El cost de la solució proposada no pot suposar més de 10.000€.

Es poden afegir altres objectius amb menys rellevància en el projecte:

- Conèixer els processos per a determinar el tipus de solució implementar.
- Conèixer els mètodes per crear escenaris propis virtualitzats.
- Identificar els diferents mecanismes que possibiliten que els convidats virtualitzats es comuniquin amb les interfícies de xarxa.
- Conèixer diferents àmbits on aplicar els escenaris virtualitzats.

1.3 Enfocament i mètode seguit

El principal propòsit d'aquest treball s'enfoca cap a la renovació d'una infraestructura obsoleta amb baix pressupost. La solució s'ha d'ajustar a les necessitats per a resoldre el problema, En concret, cal que la solució correcta s'ajusti a l'objectiu d'augmentar el temps en que triga el maquinari en trobar-se obsolet.

En primer lloc s'analitza que tipus de política permet realitzar aquesta solució amb garanties, es compara la possibilitat d'utilitzar una política de continuïtat amb la implementació d'un escenari virtual. S'analitzen les diferents tecnologies de virtualització per trobar certs mecanismes que faciliti la tasca de trobar la solució al problema de forma de confiança i amb un cost més baix.

S'intenta afegir elements que aconseguixin rebaixar el cost i aconseguir que la durabilitat del maquinari augmenti, com per exemple el programari lliure. Es defineixen tots els elements que componen la solució de manera justificada, i es detalla implementació d'aquestes tecnologies.

Finalment es realitza la valoració econòmica per visualitzar si el resultat s'ajusta al pressupost inicial.

1.4 Planificació del Treball

- Tasca 1: Anàlisi i estudi tecnològic del Hipervisor de codi obert. Adquirir els coneixements necessaris per disposar de diferents Hipervisors de codi obert capaços d'allotjar diferents tipus de màquines virtuals.
- Tasca 2: Anàlisi i estudi tecnològic de la virtualització de la xarxa. Adquirir els coneixements necessaris per disposar de diferents virtualitzadors de xarxa de codi obert capaços de donar servei a qualsevol Hipervisor.
- Tasca 3: Anàlisi i estudi de la integració d'ambdues tecnologies. Adquirir els coneixements necessaris per determinar que combinació de les dues tecnologies resolen o permeten la configuració òptima i el funcionament de la forma més òptima per al nostre propòsit.
- Tasca 4: Estudi de l'entorn virtualitzat. Adquirir els coneixements i realitzar les proves adients per permetre connexions entre l'entorn virtual.
- Tasca 5: Estudi de connexions físiques a l'entorn virtualitzat. Adquirir els coneixements i realitzar les proves adients per permetre connexions entre l'entorn virtual i l'entorn físic.
- Tasca 6: Proves de funcionament amb elements físics interns. Ampliar rols de servidor y intercalar un Tallafoc en mig.
- Tasca 7: Proves de funcionament amb elements físics exteriors. Possibilitat de aplicacions per accés remot extern entre les diferents xarxes.
- Tasca 8: Avaluar la funcionalitat del treball i dels resultats obtinguts. Definir el funcionament i determinar les funcionalitats mitjançant un cas real d'us.

Fase	Tasques	Data inici	Duració	Data final
Fase 1	Pla de treball	20/02/2019	16	08/03/2019
	Entrega PAC 1	08/03/2019		08/03/2019
Fase 2	Estudi hipervisor de codi obert.	09/03/2019	6	15/03/2019
	Estudi virtualització de la xarxa.	16/03/2019	6	22/03/2019
	Anàlisi de la integració.	23/03/2019	5	28/03/2019
	Estudi de l'entorn virtualitzat.	29/03/2019	6	04/04/2019
	Estudi de connexions físiques.	05/04/2019	7	12/04/2019
	Entrega PAC 2	12/04/2019		12/04/2019
Fase 3	Proves amb elements físics inters.	13/04/2019	12	25/04/2019
	Proves amb elements físics exteriors.	26/04/2019	12	08/05/2019
	Evaluació dels resultats obtinguts.	09/05/2019	8	17/05/2019
	Entrega PAC 3	17/05/2019		17/05/2019
Fase 4	Docum. Resultats obtinguts	18/05/2019	9	27/05/2019
	Realització de la Memòria de TFG	28/05/2019	15	12/06/2019
	Entrega Final	12/06/2019		12/06/2019

Figura 1. Tasques del TFG



Figura 2. Diagrama de Gantt del TFG

1.5 Breu descripció dels altres capítols de la memòria

- Dins el *capítol 2* es descriuen les tecnologies de virtualització de diferents distribucions y sistemes operatius.
- En el *capítol 3* es fa un petita descripció de les diferents tecnologies de virtualització de xarxes.
- Es mostra en el *capítol 4* les circumstàncies de una infraestructura informàtica obsoleta. Punt de partida que provoca la creació del projecte.

- Al *capítol 5* s'analitzen les diferents alternatives que permeten revertir les circumstàncies inicials que porten a la creació del projecte. Es compara la política de continuïtat amb la virtualització del maquinari.
- Al *capítol 6* es detalla el model a implementar mitjançant la virtualització.
- Al *capítol 7* es justifiquen la utilització de les diferents tecnologies que permeten comunicar la creació del escenari. Programari lliure, Servidor de Virtualització, Hipervisor, Maquinari virtualitzat i connectivitat de les màquines virtuals.
- Al *capítol 8* es detalla la base de la configuració del Servidor de Virtualització.
- Finalment en el *capítol 9* es realitza un valoració econòmica del projecte, es desglossen els materials necessaris per realitzar la solució i els costos derivats del personal. Es dona la avaluació del cost total del projecte.

2 Tecnologies de virtualització de maquinari

2.1 Repàs a la història de la virtualització.

Encara que la tecnologia de virtualització data de la dècada dels seixanta del segle passat, es va començar a utilitzar més àmpliament a principis del segle vint-i-un. En un inici va permetre que molts usuaris accedissin simultàniament a computadors que realitzaven processament per lots. Durant les dècades posteriors, van sorgir altres solucions que responien al problema de tenir un gran quantitat d'usuaris i una sola màquina, però així i tot, la virtualització no va seguir els mateixos passos.

Cap a la dècada dels noranta, moltes empreses tenien servidors físics i piles IT d'un sol proveïdor, la qual cosa no permetia que les aplicacions heretades s'executessin en un maquinari d'un altre proveïdor. A mesura que les empreses actualitzaven els seus entorns informàtics amb servidors bàsics, sistemes operatius, aplicacions menys costoses i de diferents proveïdors, el maquinari físic s'utilitzava de manera insuficient i cada servidor podia executar només per a una tasca específica.

En aquest moment, la virtualització va fer un veritable enlairament. Va resultar ser la solució natural per a dos problemes: les empreses podien dividir els servidors i es podia executar aplicacions heretades en diversos tipus i en diferents versions de sistemes operatius. Aquests servidors es van començar a utilitzar més i es van reduir els costos relacionats amb les compres, la instal·lació, la refrigeració i el manteniment. L'aplicació generalitzada de la virtualització va ajudar a reduir la dependència d'un sol proveïdor i va constituir la base del 'cloud computing'.

Actualment, el seu ús s'ha expandit tant en les empreses, que sovint es necessita un programari de gestió de virtualització especialitzat per a realitzar el seguiment dels convidats instal·lats. Els maquinaris moderns son prou poderosos i capaços de executar moltes instàncies de sistemes operatius independents.

2.2 Característiques de la virtualització

La virtualització és una tecnologia que té un concepte simple i un impacte profund en els centres de dades empresarials. El seu propòsit és executar una instància de sistema operatiu i una aplicació per servidor que permeti executar diverses peticions del sistema operatiu i càrregues de treball associades en un únic servidor físic. Cal agregar una capa de programari, coneguda com Hipervisor o Monitor de Màquina virtual,

La virtualització agafa un dispositiu físic i el divideix en dos, la qual cosa permet que múltiples sistemes operatius i múltiples aplicacions completes aprofitin la potència

informàtica subjacent. Es poden combinar múltiples aplicacions en una sola peça de maquinari, reduint així el nombre total de servidors necessaris, per exemple la infraestructura utilitzada en un centre de dades. Menys servidors, menys bastidors, menys equip de xarxa. Tot es tradueix en estalvis de diners, optimitzant l'espai físic i reduint els costos de manteniment.

Es redueix la necessitat de despeses en maquinari nou. Els avenços en l'automatització permeten iniciar una màquina virtual en qüestió de segons i moure diverses càrregues de treball en resposta a les canviants necessitats del negoci. El Hipervisor o monitor de màquina virtual es situa entre el sistema operatiu host i la capa de maquinari subjacent. Proporciona els recursos necessaris per executar els sistemes operatius convidats.

Els recursos es divideixen segons les necessitats de l'entorn físic i el tipus d'entorn virtualitzat. Els usuaris poden interactuar i executar processos dins del context virtual a través de la màquina virtual. El convidat funciona com un arxiu de dades únic, igual que qualsevol arxiu digital, i es pot obrir en qualsevol computadora i preveure que funcioni de la mateixa manera.

La virtualització modifica el sistema operatiu convidat abans de la instal·lació en la màquina virtual. Això millora el rendiment ja que el sistema operatiu allotjat es comunica directament amb l'Hipervisor i elimina la sobrecàrrega de l'emulació. També s'utilitza la virtualització assistida per maquinari per a reduir la sobrecàrrega del Hipervisor, però ho fa a través d'extensions de maquinari, en lloc de modificacions de programari.

2.3 Pros i contres actuals en la tecnologia de la virtualització

La **consolidacions de servidors** redueix les despeses de capital, les despeses de recursos materials i les despeses d'operacions, provoca que es puguin executar els mateixos processos amb menys servidors físics. Per tant, si un servidor físic no és configurat de la manera correcta o és atacat, podria afectar molts més servidors virtuals.

Augmenta la **velocitat d'implementació de servidors virtuals**, ja que tot es pot fer o canviar extremadament més ràpid. El cicle d'implementació de nous servidors virtuals pot realment reduir-se a dies, a minuts, o fins i tot, a segons. Però també hi ha la necessitat de mitigar el risc d'errors i evitar l'activitat maliciosa amb la mateixa rapidesa. Si les organitzacions no tenen bones pràctiques de planificació, el factor velocitat pot exacerbar les debilitats en els processos de la seva empresa. Aquest factor de velocitat en un entorn de canvi continu, pot resultar inexorablement en la manca d'entesa de l'estat actual dels actius en el seu centre de dades

A diferència d'un servidor físic, una màquina virtual és un conjunt de fitxers que resideixen físicament en un emmagatzematge compartit. Aquesta **propietat**

d'encapsulació permet mètodes molt més senzills que assegurin la continuïtat del servei. No obstant això, el tipus d'encapsulació de la màquina virtual pot oferir un nou tipus de robatori de dades. Com la màquina virtual és només un conjunt de fitxers, un servidor sencer pot ser copiat a un dispositiu USB o durant un procés de 'backup' no autoritzat.

És molt fàcil despreocupar-se de les màquines virtuals que no estan en actiu, particularment en entorns de desenvolupament. En un entorn virtual ja no existeix la relació one-to-one entre servidor físic i aplicació. En aquest moment, una màquina virtual es pot executar en qualsevol servidor físic i cada servidor físic pot tenir una gran varietat de màquines virtuals. Aquesta associació pot canviar dinàmicament mitjançant l'ús de tecnologies de migracions en calent, el que fa difícil estar al dia amb tots els canvis pel que fa a les **actualitzacions i pegats de seguretat**.

En una infraestructura física, els servidors i les xarxes són gestionades a través de nombroses aplicacions per separat. En una infraestructura virtual, els servidors i **les xarxes poden ser gestionades** pel mateix programari de la capa de virtualització. Els administradors de xarxa estan familiaritzats amb el control dels seus commutadors físics a través de l'aplicació de gestió de xarxa. Per tant, s'han d'adaptar a les noves eines de gestió i millors pràctiques en un entorn de xarxa virtual. Han d'actualitzar els seus coneixements per operar el programari de virtualització amb soltesa i evitar errors de configuració. Els riscos associats amb una mala configuració de xarxa de l'entorn virtual són molt alts i les conseqüències poden ser desastroses per al seu centre de dades .

2.4 Hipervisor

El programari denominat Hipervisor separa els recursos físics dels entorns virtuals. Prenen els recursos físics i els divideixen de manera que els entorns virtuals puguin utilitzar-los. Actualment els Hipervisores es poden classificar en dos tipus, Nadius o Allotjats.

2.4.1 Hipervisor Natiu o tipus 1

Els Hipervisores 'nadius' són una solució de programari que s'executa directament sobre el maquinari del host amfitrió, controla el maquinari i monitoritza els múltiples sistemes operatius virtualitzats que s'executen en un altre nivell per sobre del Hipervisor.

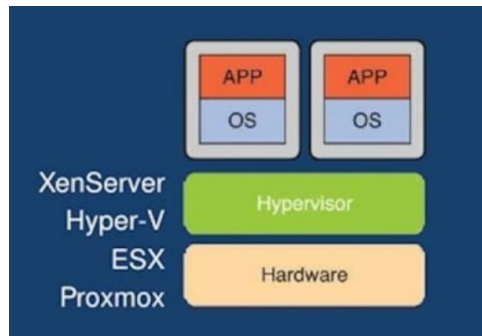


Figura 3. Hipervisor tipus 1 o natiu

La virtualització nativa utilitza una capa entremig del host físic i els màquines virtuals, i inclou codi per emular el maquinari subjacent dels convidats. Sempre que és suporti el maquinari subjacent, permet executar qualsevol sistema operatiu sense modificar. Exemples VMWare Server, XenServer, VMWare ESX.

La Paravirtualització basa en el mateix principi que la virtualització nativa amb la diferència que no inclou codi d'emulació de maquinari, i introdueix modificacions en els sistemes operatius convidats, i han de ser modificables per al pas d'instruccions privilegiades. Això millora significativament el rendiment de la virtualització. Un exemple és Xen.

Alguns dels Hipervisors de Tipus 1 més coneguts són els següents: Citrix XenServer, Citrix Hypervisor, Microsoft Hyper-V Server, Promox VEU, VMware: ESX / ESXi / ESXi Free / vSphere Hypervisor, Xen, Xtratum, encara que aquests poden ser de dos tipus: monolítics i de microkernel.

Es denomina virtualització monolítica quan una màquina virtual fa una operació amb el maquinari, i redirigeix la acció als controladors en el Hypervisor. Així és com opera VMWare, el qual utilitza molt codi per a aconseguir això. En canvi, la virtualització amb microkernel és més senzilla, ja que les màquines virtuals no necessiten controladors específics sinó que accedeixen directament al maquinari amb els mateixos controladors que usa el Hypervisor. Apareix com una capa transparent que es dedica a separar i administrar les diferents màquines virtuals. Hyper-V treballa d'aquesta manera amb un rendiment més alt.

2.4.2 Hipervisor allotjat o tipus 2

Aquests Hipervisors són una solució de programari per a virtualitzar uns altres sistemes operatius que s'executen sobre un sistema operatiu convencional, Linux, Windows, Mac OS.... D'aquesta forma la virtualització es produeix en una capa més allunyada del maquinari si ho comparem amb els Hipervisors de tipus 1.

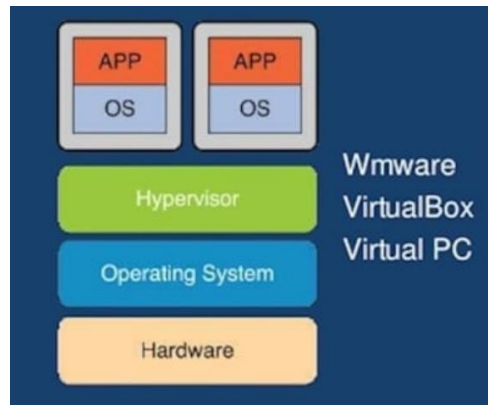


Figura 4. Hipervisor tipus 2 o allotjat

Alguns dels Hipervisors de Tipus 2 més utilitzats són els següents: Bhyve, Gnome Boxes, Kernel-based Virtual Machine (KVM), VMware: Workstation, Server, Player i Fusion, Microsoft: Virtual PC, Virtual Server, Parallels Desktop, QEMU, Red Hat Enterprise Virtualization, Sandboxie. VMLite, Virt-Manager, VirtualBox i Virtuozzo Hipervisor.

Els sistemes operatius convidats realitzen la virtualització sense utilitzar cap capa de virtualització addicional. És pot emular el maquinari a la màquina virtual o realitzar el traspàs cap a les operacions d'entrada i sortida, és l'ús directe del maquinari a la màquina virtual. VirtualBox, VMWare Player són un exemple.

La Virtualització a nivell de Sistema Operatiu realitza la virtualització sobre la màquina física, sense introduir capa intermèdia de virtualització, fent que simplement s'aïllin dins el sistema operatiu. Això limita l'ús només al mateix sistema operatiu, per exemple si pensem en Linux és podria virtualitzar totes els distribucions de Linux al S.O, però no Windows. Parlem de OpenVZ, Docker, Virtuozzo, chroot Jails i lxc com a exemples.

La Virtualització a nivell de Kernel o nucli converteix el nucli de Linux en Hipervisor, i permet executar màquines virtuals amb independència del sistema operatiu sense modificar, aquest queda emmagatzemat en una imatge de disc. Cada màquina virtual te el seu propi maquinari virtualitzat.

2.4.3 Híbrids

Com diu el seu nom, consisteix a implementar dins d'un mateix Host físic els dos tipus de Virtualització abans comentats. Aquest model és més comú per als entorns professionals, tant el sistema operatiu host com el Hipervisor corren directament en el maquinari, amb diferents nivells d'accés a diversos components de maquinari, i el sistema operatiu convidat corre sobre de la capa de virtualització. Exemple: Windows Server 2005 R2.

2.5 Tecnologies derivades

2.5.1 Virtualització en Contenedors

La virtualització basada en contenidors és una aproximació en la qual la capa de virtualització s'executa com una aplicació en el sistema operatiu. En aquest enfocament, el Kernel del sistema operatiu s'executa sobre el node de maquinari amb diverses màquines virtuals convidades aïllades. Els hosts aïllats es denominen contenidors.

Amb la virtualització basada en contenidors, no existeix la sobrecàrrega associada al mantindre cada host executant un sistema operatiu completament instal·lat. Aquest enfocament millora el rendiment perquè hi ha un sol sistema operatiu encarregant-se dels avisos de maquinari, cada convidat ha d'utilitzar el mateix sistema operatiu que utilitza el host.

En general, els entorns corporatius eviten la virtualització basada en contenidors, preferint els Hipervisors, amb l'avantatge de tenir molts sistemes operatius. Un entorn virtual basat en contenidor, és una opció ideal per als proveïdors d'allotjament que necessiten una manera eficient i segura per executar serveis. Exemples: Docker, Kubernetes, Linux-VServer, LXC, Openvz, Panamax, RKT, Singularity, Vagrant, Windows Container

2.5.2 Cloud Computing

Les xarxes de 'cloud computing' són grans grups de servidors i proveïdors de serveis que solen aprofitar la tecnologia de computació de baix cost amb connexions especialitzades per a difondre les tasques de processament de dades. Aquesta infraestructura compartida conté grans grups de sistemes que resten unificats entre si.

Les tècniques de virtualització s'utilitzen sovint per a maximitzar el poder de la computació en el núvol, la denominada 'capa en el núvol' funciona sobre un nombre de sistemes mitjançant servidors amb una versió personalitzada de Hipervisor per proveir la virtualització dels serveis. La capa controladora s'encarrega d'escalar i de gestionar la fiabilitat del sistema, i evita que els serveis es detinguin en el cas de que un servidor falli.

Es necessita un sistema operatiu especialitzat per a executar els processos i crear clústers de diversos servidors en diferents centres de dades, aquests s'encarreguen de gestionar els recursos emmagatzemats i el processament necessari per a proveir, assegurar i mantenir actius els processos de les aplicacions que es demanden. Amazon Web Services (AWS) i Windows Azure són un exemple.

3 Tecnologies de virtualització de Xarxa

La virtualització de la xarxa és un mètode per a proporcionar instàncies virtuals de xarxes físiques mitjançant la separació del ample de banda en canals independents. Cada canal pot ser assignat o reassignat de forma independent a un dispositiu en temps real. Amb la combinació d'aquests recursos, es poden aprovisionar túnels de xarxa o segments diferents, cadascun amb polítiques de gestió i d'encaminament úniques.

Està destinada a millorar la productivitat i l'eficiència mitjançant la realització de tasques de forma automàtica, permetent que els arxius, imatges i programes es puguin gestionar de forma centralitzada des d'un únic lloc físic. Els mitjans d'emmagatzematge, com discs durs i unitats de cinta poden ser fàcilment afegits o reassignats, i l'espai d'emmagatzematge també es pot compartir o reassignar entre els servidors. Es diu que la virtualització de xarxes és particularment eficaç en xarxes que experimenten augments sobtats i imprevists de dades i aplicacions que consumeixen molta capacitat.

Es poden trobar diferents tipus de tecnologies com Hipervisors de Xarxes, Commutació Virtual, Xarxes Superposades, Controladors en el Núvol, Xarxes Multi-tenant i virtualitzacions de funcions de Xarxa per realitzar la virtualització en diferents entorns.

3.1 Hipervisor de Xarxa

Un Hipervisor de xarxa proporciona una capa d'abstracció que permet aprovisionar components de xarxes virtuals o rutes que són completament independents de la xarxa física subjacent. El Hipervisor de xarxa ha de fer per la virtualització de xarxes, el que fa un Hipervisor de maquinari per a la virtualització de servidors. Habilita les aplicacions sense tenir en compte els canvis en la infraestructura subjacent.

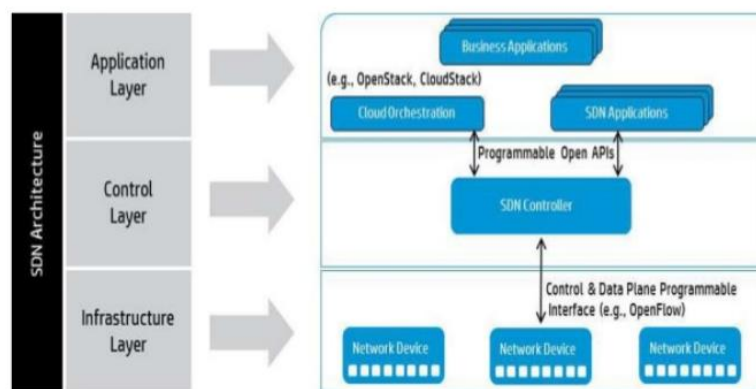


Figura 5. Arquitectura SDN.¹

¹ Enllaç figura 5: <http://luisarizmendi.blogspot.com/2013/11/software-defined-network-sdn.html>

Les xarxes definides per programari, Software Defined Networking, SDN, són un conjunt de tècniques relacionades amb l'àrea de xarxes computacionals, l'objectiu és facilitar la implementació i implantació de serveis de xarxa d'una manera determinista, dinàmica i escalable, evitant al administrador de xarxa gestionar aquests serveis a baix nivell, mitjançant la separació del pla de control, programari, del pla de dades i del maquinari.

3.2 Commutador virtual

Un commutador virtual és un exemple de programari d'un commutador físic que permet que les màquines virtuals es comuniquin entre si. Els vSwitches gestionen i dirigeixen el trànsit en un entorn virtual. Cada amfitrió virtual ha de connectar-se a un commutador virtual de la mateixa manera que un host físic es connecta a un commutador físic, es similar a un commutador Ethernet físic. Un commutador virtual no només envia paquets de dades, sinó que de forma intel·ligent encamina la comunicació a la xarxa mitjançant la inspecció dels paquets abans de reenviar.

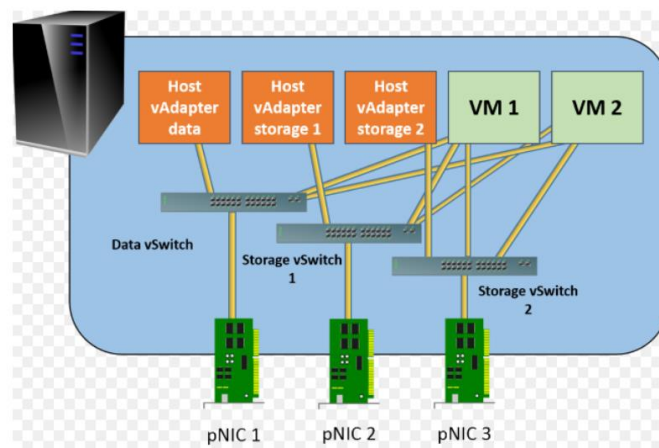


Figura 6. Commutadors virtuals²

Un commutador virtual es pot incloure en el maquinari del servidor com a part del seu firmware, però alguns proveïdors han incrustat vSwitches directament en els seus Hipervisors. La commutació virtual tradicionalment no ha estat dissenyada per presentar la visibilitat de la xarxa virtual, però eines de tercers, com el Cisco Nexus 1000v, tracten de canviar això. A més, com la commutació virtual està sota el control dels entorns SDN, els professionals de la xarxa tindran més visibilitat directa i capacitat de gestió.

3.3 Xarxa superposada, Overlay network

Una xarxa de superposició és una construcció de programari que viu a les vores d'una xarxa física i consta de commutadors virtuals que resideixen als servidors virtualitzats. Aquests commutadors s'utilitzen per crear una xarxa virtual abstracta en la

² Enllaç figura 6: <https://www.altaro.com/hyper-v/wp-content/uploads/2014/11/storage-vswitch.png>

part superior de la infraestructura física subjacent. Es basa en un pla de control de xarxa per controlar la commutació virtual als hosts de servidor, de manera similar a una xarxa física.

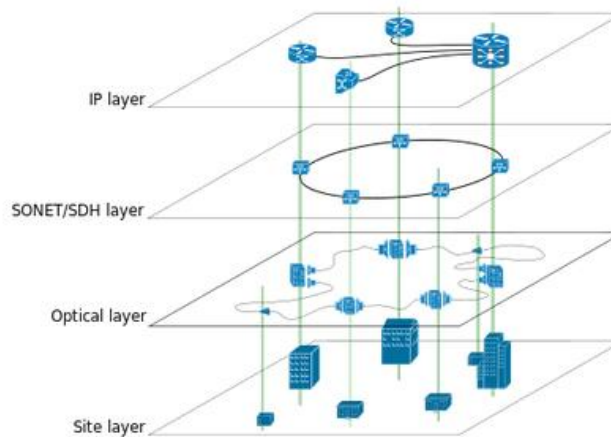


Figura 7. Estructura Overlay Network³

Aquests plans de control poden utilitzar protocols de xarxa tradicionals o poden confiar en un controlador de xarxa definit per programari. Els túnels de superposició de la xarxa fan possible la construcció d'una xarxa definida per programari a la part superior de la infraestructura física que no admet explícitament SDN.

3.4 OpenStack

OpenStack Quantum és un controlador de xarxa en el núvol i un projecte de Xarxa com a servei dins de la iniciativa de computació en el núvol OpenStack. Inclou un conjunt d'interfícies de programació d'aplicacions, plug-ins i programari de control d'autenticació i autorització que permeten la interoperabilitat i l'orquestració dels dispositius de xarxa i tecnologies en entorns IaaS.

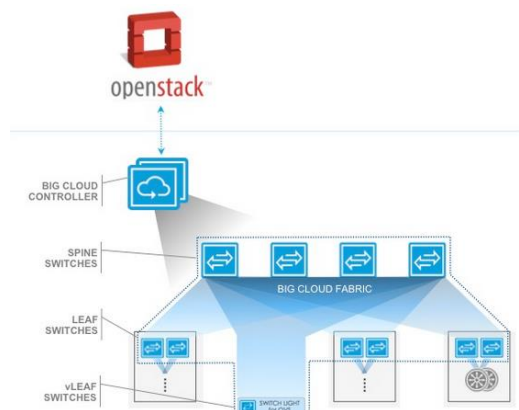


Figura 8. Open Stack, Virtual + Física⁴

³ Enllaç figura 7: https://en.wikipedia.org/wiki/Overlay_network#/media/File:Network_Overlay.svg

⁴ Enllaç figura 8: <https://www.bigswitch.com/openstack-data-centers>

L'API Quantum principal inclou suport per a les xarxes de Capa d'Enllaç i gestió d'adreces IP, així com una extensió d'una construcció per a un encaminador de Capa de Xarxa que permet l'encaminament a xarxes externes. Quantum inclou una llista cada vegada més gran del plug-ins que permeten la interoperabilitat amb diverses tecnologies de xarxes comercials i de codi obert.

3.5 Xarxes Multi Tenant

L'arquitectura de xarxa Multi Tenant permet a la xarxa física dividir-se en xarxes lògiques més petites i aïllades. Comparteixen el motor de les xarxes físiques, però funcionen amb la seva pròpia política de gestió i seguretat. Si bé la capacitat de separar les xarxes en unitats lògiques ha estat disponible des de fa algun temps a través de l'ús de xarxes VLAN, els centres de dades virtualitzats i conceptes de computació en núvol, l'han portat de tornada a l'atenció dels administradors de xarxa.

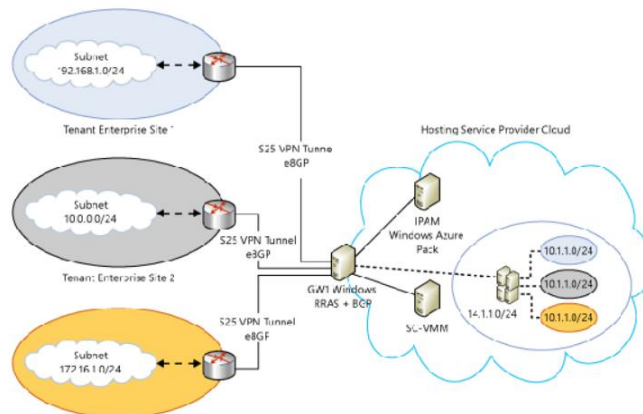


Figura 9. Esquema lògic, Xarxa Multi Tenant⁵

Les solucions Multi Tenant, estan enfocades a donar serveis a nivell de programari i maquinari a les organitzacions, en la qual múltiples empreses comparteixen el mateix recurs, per exemple la solució d'office 365. Un servidor d'Exchange permet administrar una varietat de dominis de diferents empreses en un mateix servidor.

3.6 Virtualització de les funcions de xarxa

La virtualització de les funcions de xarxa, o NFV, és una iniciativa per virtualitzar funcions de xarxa que es van dur a terme amb anterioritat per maquinari propietari i dedicat. L'objectiu de NFV és disminuir la quantitat de maquinari propietari que es necessita per posar en marxa i operar serveis de xarxa. Les funcions de xarxa que anteriorment eren fetes per encaminadors, tallafocs, balancejadors de càrrega i altres equips ara estarien allotjats en màquines virtuals.

⁵ Enllaç figura 9: <https://mountainss.wordpress.com/2013/10/11/microsoft-hybrid-cloud-multi-tenant-networking-solution-scvm-hyperv-wap-winserv/>

4 Punt de Partida

En aquest apartat es detallen les circumstàncies que obliguen a una determinada empresa a sol·licitar unes actualitzacions per a millorar la seva infraestructura informàtica, ja que en l'actualitat està deteriorant els processos productius del seu negoci. BAIXLIGHTS Sistemes de Il·luminació, empresa especialitzada en la instal·lació de sistemes de il·luminació, demanda una renovació de la seva infraestructura informàtica obsoleta.

Ens trobem amb una empresa que vol preservar la seva funcionalitat i millorar la seva productivitat sense elevar el cost en la renovació dels serveis informàtics. Les causes que han provocat aquesta sol·licitud han estat la gran quantitat de deficiències que porten arrossegant des de fa ja un temps, en aquests últims anys s'han trobat amb els següents problemes:

- Obsolescència en el maquinari, tots els servidors tenen més de cinc anys.
- Lentitud en l'execució de les tasques.
- Fallides en el Maquinari, periòdicament necessiten reiniciar els servidors per restablir el servei.
- Atacs informàtics rebuts i entrada de múltiples correus sospitosos. No es disposa de cap dispositiu de seguretat centralitzat.
- Pèrdua de suport i impossibilitat de realitzar actualitzacions per a restablir el bon funcionament del programari.
- Problemes en el moment d'introduir nous dispositius.
- Connexió a Internet lenta i problemes a l'hora de compartir arxius.
- Desconcert en el cablejat i un excés de dispositius de xarxa.
- Fallides en la connexió sense fils en la zona del taller.

No disposen de la possibilitat de realitzar una gran despesa econòmica per a la seva renovació. En la seva política d'inversions no han pogut establir el pressupost necessari que els permet establir aquesta renovació amb tecnologies més actuals, propietàries i/o capdavanteres, en aquest moment necessiten prioritzar la renovació de la maquinària del seu taller. Han especificat que el cost de la solució no els pot suposar més de 10.000 €.

A continuació es descriuen els serveis que s'executen a la actual infraestructura informàtica:

El seu petit centre de negocis està localitzat en el polígon industrial 'el Pla' i comparteixen en el mateix edifici la zona d'oficines i la zona de taller, separades per un pis d'altura. Desenvolupen la seva activitat 12 treballadors, repartits en tres departaments, administratiu, comercial i tècnic. El departament administratiu, s'encarrega de gestionar la comptabilitat, i portar al dia tota la documentació necessària per al funcionament de l'empresa; el departament comercial, s'encarrega de realitzar les visites pertinents amb els respectius clients i proveïdors; i el

departament tècnic, s'encarrega de les instal·lacions i el manteniment del sistemes de il·luminació.

- **Domini en Internet**, www.baixlights.cat
- **email**, Plataforma Google empreses amb 10 comptes de correu associades al domini www.baixlights.cat
- **Pàgina Web**, Pàgina web allotjada en el Servidor de la Xarxa Local, a través de la configuració del domini s'apunta a l'adreça estàtica de l'encaminador per a l'accés a la pàgina Web.
- **Grup de Treball**.
- **Ofimàtica**, diferents plataformes.
- **Antivirus**.
- **Plataformes de Gestió**, per al lliurament de documentació mitjançant 'https'.
- **Programes de Comptabilitat** i emmagatzematge dels documents en el Servidor de fitxers.
- **Base de dades** de proveïdors i clients.
- Diferents programes utilitzats per servei tècnic necessaris per a realitzar el manteniment.
- **Servidor FTP**. Accés als arxius necessaris per a la realització de les tasques tècniques.

L'esquema físic actual de la infraestructura:

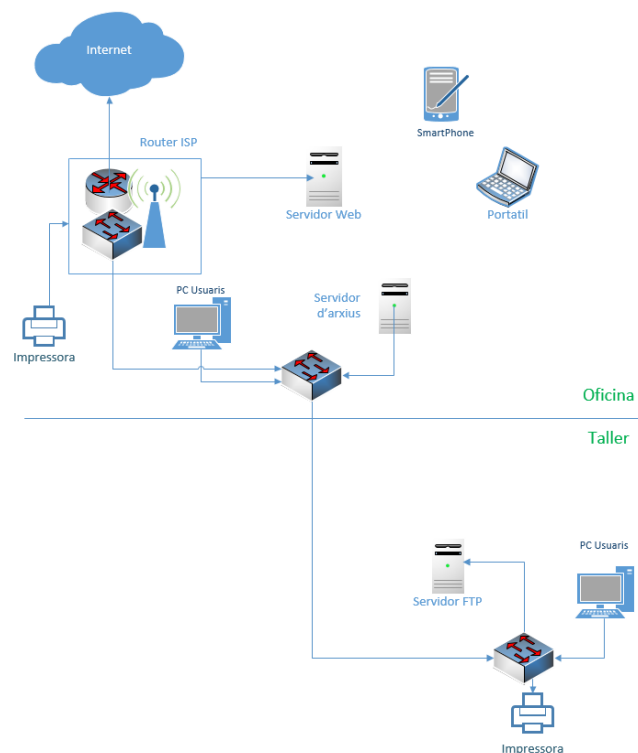


Figura 10. Infraestructura actual

La infraestructura de l'empresa es forma dels següents components:

- Servidor Windows Server 2008 en mode grup de treball per a compartir fitxers i emmagatzemar les dades dels departaments comercial i administratiu.
- Servidor Web, per a situar-se en Internet i publicitar-se.
- Servidor FTP.
- 3 commutadors per a accedir a tots els elements, es connecten totes les impressores, ordinadors personals i els servidors web, grup de treball i 'ftp' en una única xarxa local. Tots els components se situen en la mateixa subxarxa, i les connexions s'han realitzat mitjançant cablejat de Cat5e. Han afegit elements sense cap planificació en el moment concret que els han requerit.
- Encaminador ISP per a empreses, i proporciona la connectivitat 'wifi' únicament en les oficines, zona on està situat aquest encaminador.
- El departament administratiu empra tres ordinadors d'escriptori en l'oficina i una impressora.
- El departament comercial, disposa d'un ordinador d'escriptori i una impressora en l'oficina i un portàtil que utilitzen en les visites.
- El departament tècnic, utilitza un ordinador d'escriptori una impressora en el taller, i quatre portàtils per realitzar les diferents operacions amb els sistemes de il·luminació en les tasques de manteniment.

5 Anàlisi

Un cop exposats els detalls de la situació al punt de partida, s'identifiquen les diferents possibilitats que porten a determinar les millors opcions per resoldre la circumstància actual del client. En aquest capítol es detalla l'anàlisi de les vies que permeten solucionar els problemes de la obsolescència del maquinari. S'enfoquen les solucions cap a una política de continuïtat, amb la reposició del maquinari obsolet, o la utilització de maquinari virtualitzat.

A continuació es repassa els problemes derivats de la utilització de la infraestructura obsoleta, els mecanismes de la política de continuïtat i la política de virtualització, i finalment la valoració o justificació de la solució triada.

5.1 Problemes derivats de la utilització de infraestructura obsoleta

Com a punt de partida cal cerciorar-ne dels inconvenients causats per la utilització de maquinari, programari i dispositius de xarxa obsolets, alguns problemes que poden aparèixer són els següents:

- **Lentitud en l'execució dels processos d'informació.** Les últimes versions sempre compten amb un millor processament, mentre que l'ús de programari obsolet no assegura el millor acompliment, ja que les versions actualitzades ofereixen millores i major eficiència.
- **Alta vulnerabilitat i falta d'actualitzacions.** Quan més antiga és una versió de programari, més temps tenen els 'hackers' per a trobar les àrees vulnerables dins de la plataforma. En general quan es descobreixen aquestes àrees d'oportunitat són immediatament pegades pel desenvolupador per a evitar riscos, aquests pegats són alliberats amb les actualitzacions, utilitzar una versió de programari obsolet limita l'accés a aquestes.
- **Pèrdua de suport.** Els usuaris no es beneficien de les actualitzacions de seguretat i avisos llançats pel desenvolupador, mentre que els usuaris de versions actualitzades sí. Les noves vulnerabilitats no es recullen, i no és possible informar-les perquè siguin analitzades. En conseqüència, el programari obsolet és un blanc perfecte d'amenaques que posen en risc la informació i seguretat dels equips.
- **Incompatibilitat amb el maquinari.** Les noves versions d'equips poden presentar problemes o incompatibilitat amb sistemes operatius obsolets, la qual cosa significa la possibilitat de falles, suspensió de l'ajuda i garantia dels dispositius existents. És recomanable mantenir els sistemes actualitzats per a prevenir que irrompin en les dades de l'empresa, també és necessari migrar a versions vigents de programari per a evitar els riscos esmentats anteriorment.

- **Mala distribució de la xarxa.** Genera connexions als dispositius que no aprofiten totes les capacitats reals que ofereixen aquests dispositius. Una xarxa informàtica ben instal·lada resol la majoria de les vegades el desordre monumental de cables que hi ha en algunes oficines.

- **Excés de dispositius.** Una mala distribució obliga a mantenir serveis que es podrien oferir d'una forma més ordenada i escaïda.

5.2 Possibles solucions

Per a oferir una solució de forma correcta, en primer lloc cal realitzar un repàs als serveis que en aquest moment s'estan executant a la empresa, i contemplar la possibilitat d'afegir uns altres que resolguin les mancances de la infraestructura actual. Caldrà realitzar o oferir una solució que ens permeti oferir el següent escenari, òptim per al funcionament de una petita xarxa local en un àmbit de producció:

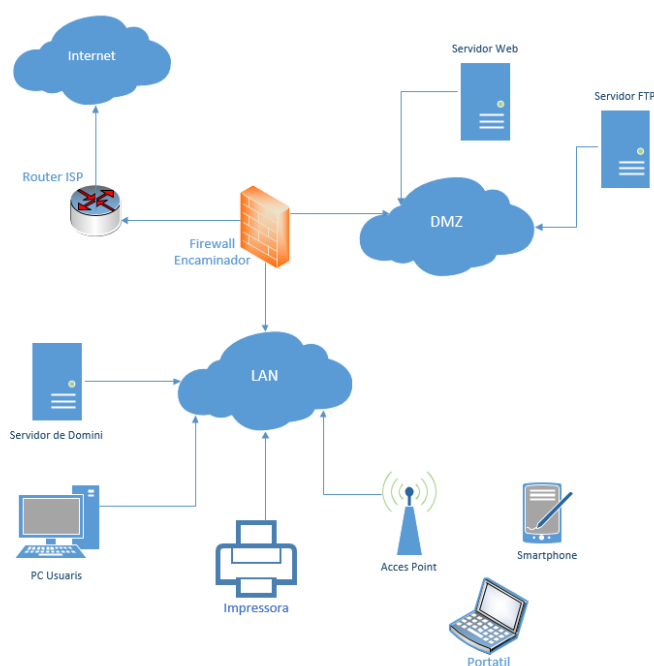


Figura 11. Esquema lògic de la de la proposta

A continuació es detallen els serveis que ha d'oferir la nova Infraestructura de Xarxa:

- **Domini en Internet** – Servei per la localització de la pàgina Web encarregada de oferir la promoció de la empresa, aquest servidor s'ubica dintre de la xarxa local.
- **Servidor Web** - La Pàgina web allotjada en un servidor dintre de la zona desmilitaritzada de la infraestructura.

- **Servidor FTP** - El departament tècnic emmagatzema els arxius necessaris per a realitzar les diferents tasques. Els operaris es connecten des de l'exterior per descarregar les configuracions dels dispositius de control dels sistemes de il·luminació. Aquest dispositiu també s'allotja dintre de la zona desmilitaritzada de la infraestructura.
- **E-mail** – Es tracta d'un servei a través d'una plataforma en el núvol, cal comprovar que els clients instal·lats en les estacions de treball poden accedir a Internet a través dels ports utilitzats per a realitzar aquests serveis.
- **Ofimàtica** - Els programes utilitzats per a realitzar aquests serveis es mantindran, per exemple, el programa client utilitzat per a enviar i rebre correu podrà configurar-ne en qualsevol aplicació, ja sigui de codi lliure o codi propietari.
- **Plataformes de Gestió** - Mitjançant el protocol 'https' es realitza el traspàs de documentació a les plataformes dels diferents organismes i entitats. L'enviament d'aquesta documentació es realitza a través de l'explorador web.
- **Estacions de treball** - Es mantenen els maquinaris i s'oferiran tots els serveis capaços d'executar-se des de qualsevol plataforma, d'aquesta manera no serà necessària la seva renovació.
- **Tallafocs** – Element a afegir per aportar més seguretat als elements que componen la infraestructura. Es vol evitar l'accés a la xarxa per protegir-la d'accessos malintencionats i proveir de seguretat a l'equipament accessible des de Internet.
- **Punts d'accés sense fils** - Es necessiten dos dispositius per la connexió sense fils a la zona d'oficines i al taller.

5.2.1 Solució mitjançant una política de continuïtat

Aquest tipus de solució es basa en la idea de substituir el maquinari obsolet per un altre amb característiques més modernes i actualitzades. En aquest sentit es necessari identificar quins són elements que necessiten una reposició i identificar totes les actualitzacions i els nous equips a instal·lar.

En un primer moment es pot preveure la quantitat de nous recursos i la adquisició de llicències que es necessiten per actualitzar els serveis en el nou maquinari mitjançant una política de continuïtat. En aquest tipus de solucions calen renovacions del programari per que els nous maquinaris optimitzin les funcions del sistema operatiu allotjats.

- Es necessita un maquinari per allotjar una versió actualitzada del **Servidor Windows Server 2008** com Controlador de Domini, amb la conseqüència de tindre que contractar una llicència d'us per el propietari d'aquesta distribució.
- Un maquinari nou per ubicar un **Servidor Web**. Per mantindre aquest servei en necessari l'actualització del sistema operatiu i cal contractar una nova llicència.

- Un maquinari nou per ubicar un **Servidor FTP**. Per aquest servei es podrà utilitzar el programari existent, ja que el servei es pot oferir des de qualsevol plataforma.
- substituir el tres **commutadors** per dispositius més actualitzats que permetin la connectivitat entre els diferents elements de la xarxa.
- Incloure un **Tallafocs** mitjançant maquinari, aquest dispositiu necessita un mínim de tres interfícies de xarxa.
- Es necessiten dos **Punts d'Accés** per la connexió sense fils a la zona d'oficines i al taller. Aquest dispositius obtindran la seva connectivitat a partir del nou commutador.

Calen tres nous servidors per substituir el maquinari obsolet, un d'ells de gamma empresarial, el Servidor Web i el Servidor FTP poden ser servidors d'escriptori. Es necessari incloure un dispositiu amb el rol de Tallafocs, encara que existeixen diferents models dedicats per aquesta funció, no cal que sigui un altre servidor.

El canvi dels tres commutadors de xarxa suposarà una millora en la velocitat de connexió dels diferents dispositius, i amb els dos nous punts d'accés es connecten els dispositius mòbils de l'oficina i del taller.

5.2.2 Solució mitjançant la virtualització

Per a poder aplicar una solució a aquesta problemàtica, dins aquest àmbit, amb garanties i a baix cost, és necessari plantejar la virtualització dels equips físics en lloc de la reposició per màquines amb millors característiques. A través d'un servidor de virtualització s'emula el funcionament d'una infraestructura de servidors real, i es proporciona un entorn d'execució idèntic al físic.

Amb un servidor de virtualització es redueix els recursos aplicats a la infraestructura física. S'elimina la necessitat de substituir els servidors físics i es veuen reduïts els requisits immobiliaris, d'alimentació i refrigeració, amb la consegüent i important disminució dels costos.

Al agrupar, ordenar, ampliar i reestructurar tots els recursos en un sol servidor, es rebutja el model heretat de una aplicació per a un servidor. Es pot gestionar tota la infraestructura i garantir la reducció dels costos dedicats a tasques repetitives de configuració, supervisió i manteniment.

S'augmenta la disponibilitat de les aplicacions reforçant la continuïtat del negoci. S'eliminen les parades planificades i es pot efectuar una recuperació ràpida en el cas de rebre un imprevist en el subministrament elèctric. Es tindrà la capacitat de realitzar còpies de seguretat de forma segura i es podrà migrar la totalitat dels entorns virtuals sense interrupció del servei.

- **Servidor Web.** Cal traspasar al nou sistema operatiu allotjat tots els arxius que el configuren. S'haurà de permetre l'accés des de l'exterior i serà necessari aplicar noves directives per a poder accedir.

- **Servidor FTP.** El servidor passarà a ser una nova màquina virtual. Cal traspasar tots els arxius al nou sistema operatiu allotjat, i permetre l'accés des de l'exterior aplicant noves directives per a poder accedir.

- **Grup de Treball.** Actualment, el grup de treball és utilitzat com a servidor de fitxers que permet l'emmagatzematge de carpetes compartides. Aquest servidor passarà a ser una nova màquina virtual i necessita una distribució que emuli els serveis de controlador de domini. Cal proporcionar tot el necessari perquè els departaments d'administració i comptabilitat mantinguin l'accés a tots els arxius existents.

Per aplicar esta política caldrà nous elements per la construcció de la nova infraestructura:

- **Servidor de virtualització** - Es el maquinari on s'instal·len les noves màquines virtuals, tindrà prou memòria per córrer almenys quatre màquines virtuals, i dos interfícies físiques de xarxa per les connectivitats físiques. La seva ubicació serà al nou rack de comunicacions.

- **Rack de comunicacions** - la principal raó que dur a terme la instal·lació d'un nou armari, es que actualment l'empresa disposa d'un petit rack mural en el qual no es poden afegir nous elements. A causa d'aquest fet, i juntament amb els problemes creats per la mala infraestructura física de la xarxa, es decideix renovar el cablejat estructurat de cat5 per cablejat estructurat de cat6. Es centralitzen les connexions de tots els dispositius i s'inclouen alguns nous punts de connexió, per exemple, per ubicar els nous punts d'accés sense fils.

- **Commutador de xarxa gestionat** - Amb el commutador es centralitzen i s'unifiquen tots els elements de xarxa existents, s'instal·la en el nou Rack de Comunicacions i té la capacitat per donar connectivitat a tots els elements físics de la infraestructura.

- **Distribucions de programari** - A banda del sistema operatiu per l'Hipervisor, caldrà virtualitzar un Tallafoç, element encarregat de realitzar l'encaminament entre les diferents xarxes creades dintre del Servidor de Virtualització. Dues màquines virtuals més que substituiran al servidor FTP i al servidor Web, i el nou servidor de Domini utilitzat per la gestió dels diferents usuaris dins la xarxa.

- **Punts d'accés sense fils** - Es necessiten dos dispositius per la connexió sense fils a la zona d'oficines i al taller.

- **Emmagatzematge connectat a la xarxa, NAS** – Necessari per crear còpies de seguretat, tant dels fitxers del usuaris com del servidor de virtualització. La seva ubicació també serà al nou rack de comunicacions.

5.3 Justificació de la solució triada

Una vegada exposades les dues possibilitats per a realitzar la implementació de la solució, Es pot decidir d'una manera més objectiva si cal realitzar una política de continuïtat o decantar-nos per la virtualització del maquinari. Les diferents raons que han portat a realitzar la solució mitjançant la virtualització queden indicades a continuació.

En referència als costos del material, continuar mitjançant una política de continuïtat amb l'objectiu de reemplaçar tot el maquinari obsolet, suposa una despesa excessiva. Cal adquirir tres servidors nous, un de gamma empresarial i un dispositiu que faci de Tallafocs. Mitjançant la virtualització, encara que el servidor de virtualització segurament tingui un cost més alt, aquest permetrà pràcticament estalviar els costos de la reposició del maquinari utilitzat per als servidors DMZ , FTP i els costos de l'adquisició del Tallafocs.

En referència a la implementació o posada en marxa del sistema, és cert que la virtualització necessita més temps per a la seva implementació, el personal informàtic necessita més temps per a construir l'escenari. Aquesta circumstància pot quedar compensada si es compara amb la obligació que ofereix la política de continuïtat en l'adquisició de noves llicències per executar-se en el nou maquinari.

En referència a la durabilitat del maquinari, el maquinari utilitzat en la política de continuïtat té una durabilitat aproximada de tres a cinc anys, a partir d'aquest temps cal tornar a plantejar canviar el maquinari de nou. Per contra, mitjançant la virtualització, utilitzant un servidor de virtualització de gamma alta podem arribar a mantenir els serveis uns vuit anys.

6 Model

El servidor de virtualització es converteix en el centre neuràlgic de la infraestructura. Per una banda es creen les diferents xarxes de l'escenari i es controlen totes les interfícies de xarxa, i per l'altre, s'ubiquen les màquines virtuals dels principals equips de la infraestructura.

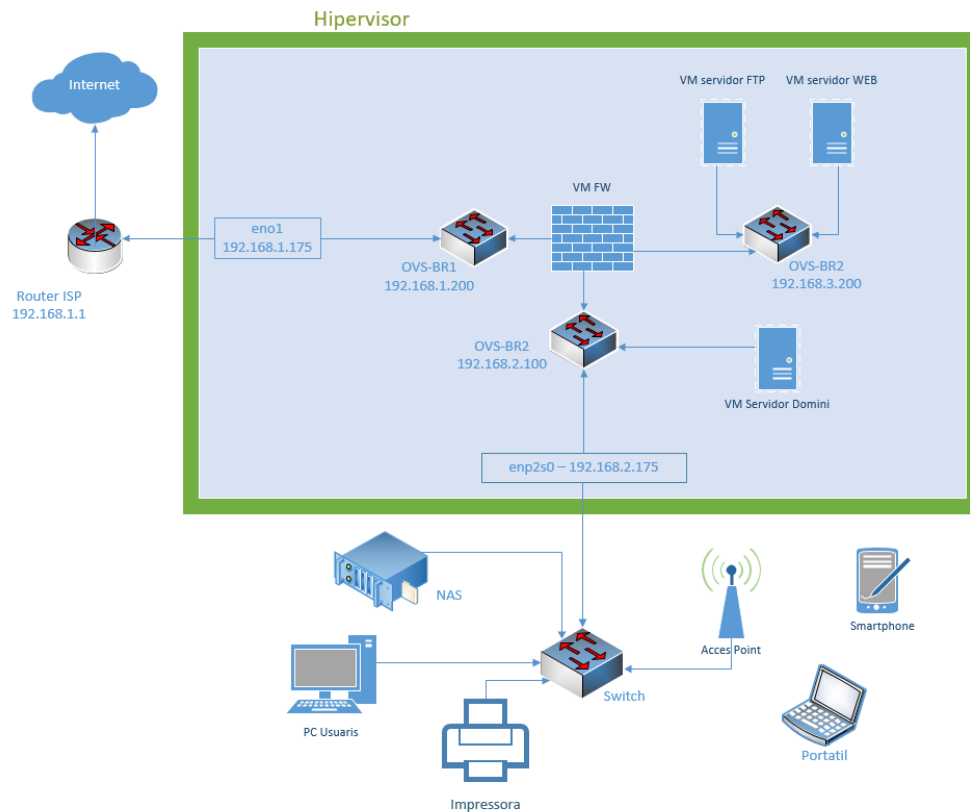


Figura 12. Esquema del model

Es creen els diferents **commutadors virtuals** dintre del servidor virtualització, i s'estableixen els commutadors de les tres xarxes del escenari, un commutador per la connectivitat cap a l'exterior o Internet, un altre per la connectivitat dels diferents elements de xarxa local i un altre per la connectivitat dels servidors ubicats a la zona desmilitaritzada. En un primer moment, els commutadors virtuals queden aïllats de la part física de la infraestructura.

S'utilitzen 'bridges' per realitzar les **connexions de les interfícies físiques** cap als diferents commutadors virtuals. Un cop s'estableix la connexió entre les diferents interfícies físiques amb el corresponent commutador virtual es permet la connectivitat amb el enrutador i el commutador físic de la xarxa local. Amb aquesta operació queda habilitada la connectivitat dels elements físics amb la virtualització.

Quatre son les diferents màquines virtualitzades dins de l'Hipervisor, En primer lloc es virtualitza el **Tallafocs**, ja que és el dispositiu que permet la connectivitat i l'encaminament de tots els dispositius entre les diferents xarxes, dins d'aquesta màquina virtual estan creades les portes d'enllaç que utilitzen els diferents dispositius a les seves configuracions de xarxa. La configuració del Tallafocs permet la connectivitat entre la xarxa local i l'encaminador de sortida cap a Internet, i aïlla el Servidor Web i Servidor FTP de la resta.

Els elements de la zona desmilitaritzada, **Servidor Web** i **Servidor FTP**, queden totalment virtualitzats, la comunicació amb l'entorn físic es fa a través del Tallafocs mitjançant el commutador virtual destinat per la DMZ. Es mantenen separats de la xarxa local per evitar problemes a l'hora d'executar programari o accedir a determinats serveis des de l'exterior.

El **Servidor de Domini** permet administrar els principals serveis de la xarxa local, com l'accés a Internet i la compartició de recursos. La seva estructura jeràrquica permet mantenir una sèrie d'objectes relacionats amb els components de una xarxa, com a usuaris, grups d'usuaris, permisos i assignació de recursos. Aquesta màquina virtual es connecta directament amb el commutador virtual de la xarxa local.

La comunicació física per a la xarxa local es realitza a través d'un **Switch físic configurable** i la interfície física de l'Hipervisor prèviament definida. Aquesta característica també pot ser vàlida per passar diferents xarxes virtuals des del Hipervisor a través d'una interfície física del servidor de virtualització.

A través del commutador físic i els **punt d'accés sense fils** connectem la resta del elements de la xarxa local que conformen la infraestructura. Estacions de treball, Impressores, dispositius mòbils, i finalment amb al **NAS** element físic que s'utilitza per a albergar les còpies de seguretat de tots els arxius, documents, bases de dades i la imatge del servidor de virtualització.

7 Justificacions

Un dels objectius inicials d'aquest treball és concebre un mètode mitjançant programari de codi obert que permeti albergar i crear una infraestructura virtualitzada capaç de comportar-se com a element principal de petits centres de producció.

En aquest apartat s'intenta localitzar i diferenciar les tecnologies que permeten comunicar les màquines virtuals dins l'Hipervisor i les tecnologies seleccionades per crear l'escenari. Es troben de forma detallada les raons que han portat l'elecció del Hipervisor i els elements de xarxa que permeten la creació de la nova infraestructura virtualitzada. Es repassen les diferents particularitats, el funcionament i els protocols utilitzats en els projectes de codi obert existents.

7.1 Programari Lliure

Amb l'objectiu d'adaptar i optimitzar encara més els costos de la solució exposada al pressupost, es proposa la utilització de codi lliure per realitzar el procés de virtualització en lloc de utilitzar solucions de codi propietari.

El Programari Propietari es refereix a qualsevol programa informàtic en el qual els usuaris tenen limitades les possibilitats d'utilitzar-lo, modificar o redistribuir-lo, el codi font no està disponible o el seu accés es troba restringit. Al programari propietari, una persona física o jurídica posseeix els drets d'autor per utilitzar el programa amb qualsevol propòsit. No es pot estudiar com funciona el programa i no es pot adaptar a les pròpies necessitats. D'aquesta manera un programari continua com a propietari, tot si el codi font es fa públic i es reserven els drets sobre l'ús, modificació o distribució.

Desavantatges més significatius del programari propietari

- És il·legal fer còpies del programari propietari sense abans haver contractat les llicències necessàries.
- En la majoria dels casos el suport tècnic és insuficient o triga massa temps a oferir una resposta satisfactòria.
- És il·legal estendre una peça de programari propietari per a adaptar-la a les necessitats particulars d'un problema específic.
- La innovació és dret exclusiu de la companyia, si algú té una idea innovadora respecte a una aplicació propietària, ha de triar entre vendre-li la idea a la companyia propietària de l'aplicació o escriure des de zero la seva pròpia versió d'una aplicació equivalent.
- És difícil aprendre a utilitzar eficientment el programari propietari sense haver assistit a costosos cursos de capaciació.

Avantatges més significatius del programari propietari.

- Es destina una part important dels recursos a la recerca sobre els usos del producte.
- Existeix programari propietari dissenyat per a aplicacions molt específiques que no es troba en cap altre lloc més que amb la companyia que el produeix, es desenvolupa programari per a aplicacions molt específiques.
- Existeix gran quantitat de publicacions, àmpliament difoses, que documenten i faciliten l'ús de les tecnologies proveïdes per companyies de programari propietari, encara que el nombre de publicacions orientades al programari lliure va en augment.

Desavantatges més significatius del programari lliure.

- El programari lliure no té garantia provinent de l'autor i s'adquireix sense garanties explícites del fabricant.
- Es necessita dedicar recursos a la reparació d'errors. No obstant això en el programari propietari és impossible reparar errors, cal esperar que treguin a la venda una altra versió.
- No existeixen companyies úniques que recolzin tota la tecnologia.
- La majoria de la configuració de maquinari no és intuïtiva. Es requereixen coneixements previs sobre el funcionament del sistema operatiu i fonaments de l'equip a connectar per a aconseguir un funcionament adequat.
- L'usuari ha de tenir nocions de programació, l'administració del sistema recau molt en l'automatització de tasques.
- En sistemes amb accés a Internet, s'han de monitoritzar constantment les correccions d'errors de tots els programes que continguin aquests sistemes, ja que són fonts potencials d'intrusió.
- La diversitat de distribucions, mètodes d'empaquetament, llicències d'ús, eines amb una mateixa fi, etc., poden crear confusió.

Avantatges més significatius del programari lliure

- Requisits de maquinari menor i durabilitat de les solucions, els sistemes Linux que actuen de servidors poden ser utilitzats sense la interfície gràfica, amb la conseqüent reducció de requisits de maquinari necessari.
- Baix cost d'adquisició i lliure ús, ja que el programari, com a mercaderia, en general no està a la venda, el que l'usuari adquireix és una llicència respecte dels usos que pot donar als programes en qüestió.
- El programari lliure garanteix una independència respecte al proveïdor gràcies a la disponibilitat del codi font. Qualsevol empresa o professional, amb els coneixements adequats, pot continuar oferint desenvolupament o serveis per a la nostra aplicació.
- Ofereix privacitat i seguretat, les dades personals no estan en el costat del propietari.

El Programari Obert o de codi lliure vol dir distribuir, modificar, copiar i utilitzar. Per tant cal comptar amb un codi font per a fer-ho efectiu, i es necessari que el programa sigui gratuït. El programari de codi lliure permet executar un programa per al nostre propòsit, estudiar i adaptar el seu funcionament, millorar-lo, redistribuir còpies, i es pot

publicar per a tota la comunitat. La llibertat per a utilitzar un programa significa que qualsevol altra organització pot executar-lo des de qualsevol altre sistema informàtic, i haurà de ser lliure per a les modificacions introduïdes i integrades de forma privada.

7.2 Elecció del Hipervisor.

7.2.1 Principals proveïdors de software de virtualizació

En el món de la tecnologia empresarial, la majoria de la informació en línia prové de proveïdors, però el que realment es valúés és la informació objectiva d'altres usuaris. Els professionals de WeightedOver, Nova York, han creat una llista de proveïdors de nivell empresarial, basada en anàlisi de productes, qualificacions i comparacions. Totes aquestes crítiques i validacions són d'usuaris reals i validades per un elaborat procés d'autenticació.

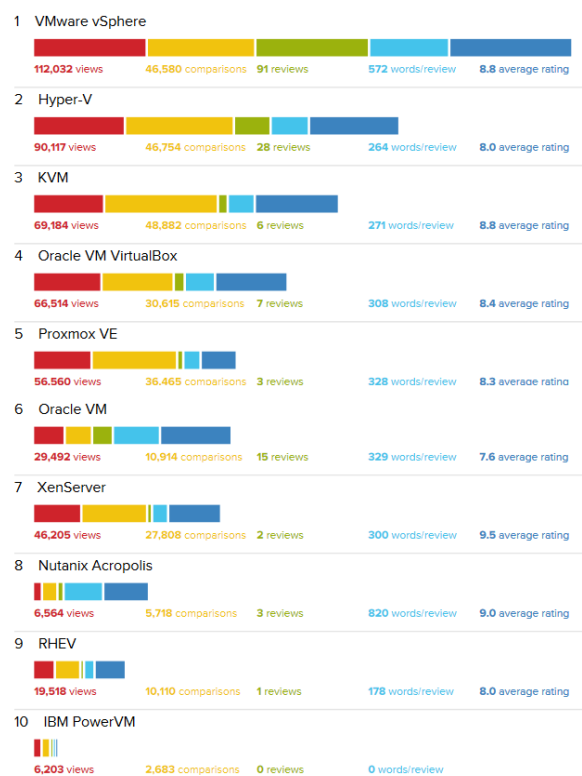


Figura 13. Valoracions de Hipervisors⁶

Els revisors d'aquests productes han estat validats com a usuaris reals en funció dels seus perfils de LinkedIn per garantir que proporcionen opinions fiables i no les dels proveïdors de productes. Les anàlisis i qualificacions dels revedors estan

⁶ Enllaç figura 13: <https://bit.ly/2MBoBNa>

excloses. La classificació total d'un producte es basa en una classificació agregada ponderada de les opinions, comparacions, comentaris d'aquest producte i una mitjana qualificació.

A partir d'aquest estudi podem comprovar que la elecció principal dels usuaris per solucions de programari propietari son VMware vShepre i HyperV, i en canvi KVM es la millor alternativa realitzada amb programari no propietari. A continuació es detallen les característiques dels principals programaris de codi lliure per la elecció del Hipervisor: VirtualBox, Xen i KVM.

7.2.2 Virtual Box

Oracle VM VirtualBox és un programari de virtualització per arquitectures x86/amd64. Actualment és desenvolupat per Oracle Corporation com a part de la seva família de productes de virtualització. Per mitjà d'aquesta aplicació és possible instal·lar sistemes operatius addicionals, coneguts com sistemes convidats dins d'un altre sistema operatiu amfitrió, cada un amb el seu propi ambient virtual.

VirtualBox s'executa en hosts de Windows, Linux, Macintosh i Solaris i admet una gran quantitat de sistemes operatius convidats, inclosos, entre d'altres, Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x i 4.x), Solaris i OpenSolaris, OS / 2 i OpenBSD.

És un potent producte de virtualització per a empreses i per a ús domèstic, no només és un producte extremadament ric en funcions i amb un alt rendiment per a clients empresarials, sinó que també és l'única solució professional que està disponible gratuïtament com a programari de codi obert segons els termes de la Llicència pública general de GNU (GPL) versió 2.

VirtualBox ofereix algunes funcionalitats interessants, com l'execució de màquines virtuals de forma remota, per mitjà del Remote Desktop Protocol i suporta iSCSI, encara que aquestes opcions no estan disponibles en totes les versions. Pel que fa a l'emulació de maquinari, els discs durs dels sistemes convidats són emmagatzemats en els sistemes amfitrions com arxius individuals en un contenidor anomenat Virtual Disk Image, incompatible amb els altres programaris de virtualització.

VirtualBox s'està desenvolupant activament amb llançaments freqüents i té una llista cada vegada més gran de característiques, sistemes operatius convidats compatibles i plataformes en què s'executa. És un esforç comunitari recolzat per una empresa dedicada, s'encoratja a tots a contribuir, mentre que Oracle garanteix que el producte sempre compleix amb els criteris de qualitat professional

7.2.3 Xen

Xen 1.0 va ser llançat oficialment el 2004, seguit de Xen 2.0. Alhora, Ian Pratt i altres líders de tecnologia es van involucrar amb l'equip del projecte. Van fundar una empresa coneguda com XenSource, que més tard va ser adquirida per Citrix per convertir l'Hipervisor d'una eina de recerca en un producte competitiu per a la informàtica empresarial. El Hipervisor va seguir sent una solució de codi obert i des de llavors s'ha convertit en la base de molts productes comercials.

En 2013, el projecte es va fer ser sota la Fundació Linux. Acompanyant al moviment, es va adoptar una nova marca registrada 'Projecte Xen' per diferenciar el projecte de codi obert dels molts esforços comercials que van utilitzar la marca registrada més antiga 'Xen'.

Es pot facilitar l'aïllament segur, el control de recursos, la garantia de qualitat de servei i la migració de màquines virtuals. Els sistemes operatius poden ser modificats explícitament per corregir Xen mantenint la compatibilitat amb aplicacions d'usuari. Això permet aconseguir virtualització d'un altre rendiment sense suport especial del maquinari. Intel ha realitzat diverses contribucions a Xen que han permès afegir un suport per a les seves extensions d'arquitectura VT-X Vanderpool. Aquesta tecnologia permet que els sistemes operatius es modifiquin actuant com a hosts dins dels màquines virtuals de Xen, sempre que el servidor físic pugui suportar les extensions VT d'Intel o Pacifica de AMD.

El paravirt_ops, o pv-ops per abreviar, és una peça de la infraestructura del nucli Linux que permet executar el nucli de forma paravirtualitzada sobre un Hipervisor. Actualment, suporta Xen, entre altres opcions de virtualització, i la infraestructura del Kernel permet compilar el mateix nucli binari que pot configurar de forma nativa en un maquinari senzill o executar-se com a nucli del domini de Xen.

7.2.4 KVM

La màquina virtual basada en el nucli és una tecnologia de virtualització de codi obert integrada a Linux®. KVM pot convertir a Linux en un Hipervisor capaç de fer que una màquina d'amfitrió executi entorns virtuals múltiples i aïllats. Es pot trobar a partir de Linux 2.6.20. A causa de que és part del codi existent de Linux, KVM aprofita de forma immediata cada nova funció, solució i progrés de Linux sense requerir enginyeria addicional.

KVM converteix Linux en un Hipervisor de tipus 1, sense sistema operatiu. Tots els Hipervisors necessiten alguns components al nivell del sistema operatiu per executar les màquines virtuals, per exemple, l'administrador de memòria, la planificació de processos, la pila d'entrada o sortida, I/O, els controladors dels dispositius, la gestió de seguretat, la pila de xarxa i més... Cada màquina virtual s'implementa com un procés regular de Linux, programada pel planificador estàndard de Linux amb maquinari virtual dedicat com a targeta de xarxa, adaptador de gràfics, CPU, memòria i discos.

KVM s'ha d'executar dintre d'una versió de Linux llançada després de 2007 i que s'hagi d'instal·lat en maquinari X86 que sigui compatible amb capacitats de virtualització, tot el que s'ha de fer és carregar dos mòduls existents, un mòdul sistema principal del nucli i un mòdul específic del processador, un emulador i qualsevol controlador que ajudi a executar sistemes addicionals.

Tot el que té Linux, KVM també el té. Però hi ha funcions específiques que fan que KVM sigui l'Hipervisor empresarial amb millor garanties de bon funcionament:

- KVM és un mòdul del Kernel que exposat en dev/kvm es pot utilitzar per a realitzar la virtualització assistida per maquinari. Això permet que les màquines virtuals aprofitin les instruccions ràpides de la CPU per a realitzar la virtualització. QEMU emula el maquinari i aprofita KVM per a executar el sistema operatiu convidat. 'Libvirt' és una API de virtualització que administra juntament QEMU+KVM per proporcionar funcions de nivell superior, com per exemple emmagatzematge i administració de xarxa.

- KVM utilitza una combinació de security-enhanced Linux, SELinux, i virtualització segura, 'sVirt', per a la seguretat i l'aïllament millorats de màquina virtual. SELinux estableix els límits de seguretat per a les màquines virtuals i sVirt amplia les capacitats de SELinux. el que permet que la seguretat de control d'accés obligatori, MAC, s'apliqui a les màquines virtuals hostes i evita els errors manuals d'etiquetatge.

- KVM pot utilitzar qualsevol emmagatzematge compatible amb Linux, inclosos alguns discos locals i l'emmagatzematge connectat a la xarxa, NAS. Les entrades y sortides de rutes múltiples millora l'emmagatzematge i proporciona redundància. També és compatible amb sistemes d'arxius compartits de tal manera que les imatges de les màquines virtuals puguin conviure entre diversos hosts.

- KVM pot utilitzar una àmplia varietat de plataformes de maquinari certificat i compatibles amb Linux. Com els proveïdors de maquinari que contribueixen de forma periòdica al desenvolupament del nucli, les funcions de maquinari més recents sovint s'adopten ràpidament en el nucli de Linux.

- KVM hereta les funcions de gestió de memòria de Linux, inclosos l'accés a la memòria no uniforme i la fusió de la mateixa pàgina del nucli. La memòria d'una màquina virtual es pot intercanviar, té el suport de grans volums per a un millor rendiment, i es pot compartir o recolzar per un arxiu de disc.

- KVM permet la migració en viu, això és la capacitat de moure una màquina virtual en funcionament d'un host físic a un altre sense que s'interrompi el servei. La màquina virtual roman encesa, les connexions de xarxa romanen actives i les aplicacions continuen executant-ne mentre es col·loca la màquina virtual. KVM també guarda l'estat actual de la màquina virtual perquè es pugui emmagatzemar i reprendre posteriorment.

- KVM hereta el rendiment de Linux, ja que es pot escalar fins a satisfer la càrrega requerida si la quantitat de màquines hostes i les demandes creix. KVM permet que les

càrregues de treball de les aplicacions més exigents es virtualitzin, és la base per a moltes configuracions de virtualització empresarial, com els centres de dades i els núvols privats.

En el model de KVM, una màquina virtual és un procés de Linux, programat i controlat pel nucli. El planificador de Linux permet el control detallat dels recursos assignats a un procés de Linux i garanteix la qualitat del servei per a un procés en particular. En KVM, això inclou el planificador complet, els grups de control, els espais de nom de xarxa i les extensions en temps real.

El nucli de Linux compta amb extensions en temps real que permeten que les aplicacions basades en màquines virtuals s'executin amb una latència més baixa i una millor prioritització enfront del Hipervisor sense sistema operatiu. El nucli també divideix els processos que requereixen llargs períodes de computació en components més petits que després es programen i es processen en conseqüència.

7.2.5 Conclusions

VirtualBox no està dissenyat per a un ús intensiu, ja que Virtualbox és un programari simple que es pot fer servir per crear màquines virtuals. És una bona opció per iniciar-se en la virtualització, en canvi, KVM és una de les aplicacions de virtualització estàndard de la indústria de codi obert més utilitzada. Pot dedicar RAM, CPU, sobrecomprimir recursos físics i escalar-se tant com es vulgui.

Actualment el projecte KVM és propietat de Red Hat, i no realitza cap emulació com la realitza VirtualBox. En el seu lloc, exposa la `/dev/kvm` interface, que es pot utilitzar per configurar l'espai d'adreces de la màquina virtual convidada. El host també ha de proporcionar una imatge de firmware, generalment una BIOS personalitzada a l'emular PC, que pot usar per iniciar el seu sistema operatiu principal.

Per altre banda, la diferència més significativa entre KVM i Xen resideix en que KVM és un mòdul més del nucli, no és un nucli diferent com ocorre Xen. Al ser un mòdul del nucli, es pot descarregar en temps d'execució suportant els altres mòduls. Xen no ve per defecte al nucli, encara que en algunes de les seves distribucions es crea un pegat al nucli per treballar amb més comoditat. Degut a que KVM es part del 'Kernel' utilitza el suport per a diferents processadors, la gestió de la memòria i l'accés a la memòria no uniforme.

Una capacitat que té KVM davant Xen, és la possibilitat de compartir pàgines de memòria. De la mateixa manera, a la part del nucli s'utilitzen menys línies de codi per a moltes funcions de l'abast del propi nucli i s'obté un desenvolupament més fàcil i centralitzat.

En aquest cas s'ha optat per utilitzar KVM, ja que és una de les millors solucions per a la virtualització dins del nucli de Linux, i amb 'libvirt', dimoni i eina de gestió per a la virtualització de plataformes, es crea una poderosa combinació per treballar en entorns de desenvolupament o producció. KVM crea i administra d'una manera

senzilla les màquines virtuals, i proporciona un kit d'eines que interactuen amb les capacitats de virtualització de les versions més recents de Linux i altres sistemes operatius.

Quan l'entorn virtual s'està executant i un usuari o programa emet una instrucció que requereix recursos addicionals de l'entorn físic, el Hipervisor transmet la sol·licitud al sistema físic i guarda els canvis en la caixa. Tot això succeeix pràcticament a la mateixa velocitat que si aquest procés es realitzés dins de la màquina física, especialment, si la sol·licitud s'envia a través d'un Hipervisor de 'open core' basat en KVM, la màquina virtual basada en el Kernel.

7.3 Sistema Operatiu per allotjar l'Hipervisor.

En aquest apartat és necessari definir l'elecció del sistema operatiu una vegada triat el Hipervisor tipus 2 de codi lliure, al ser seleccionat KVM, es adient seleccionar el sistema operatiu que millor funcioni amb aquest tipus Hipervisor.

En tractar-se KVM d'un Hipervisor allotjat, necessitem introduir una distribució Linux amb garanties. Red Hat desenvolupa el projecte KVM i liberalitza tot el codi font del producte de forma pública sota els termes de la Llicència Pública General de GNU i altres llicències a través de la distribució CentOS. Els desenvolupadors de CentOS utilitzen aquest codi font per crear un producte final compatible amb un nivell binari i funcional amb Red Hat.

Amb la distribució CentOS es pot millorar el rendiment i l'equilibri de la càrrega dels recursos que configuren els equips que funcionen de forma col·lectiva, incloent un Tallafocs potent i el mecanisme de polítiques SELinux. La distribució ofereix suport durant sis anys amb actualitzacions de seguretat i paràmetres crítics mantinguts durant una dècada després del llançament inicial.

CentOS és compatible amb l'estratègia de redistribució del proveïdor i l'obtenció del suport complet amb actualitzacions de seguretat i material de capacitació. Si està configurat correctament i s'executa en un maquinari de qualitat, és un sistema operatiu de servidor molt estable, amb problemes molt petits. Es redueix el risc de caigudes i errors, ja que executa versions de programari empaquetat.

La instal·lació de la distribució de Centos7 al maquinari del servidor es pot configurar amb maquinari de nivell empresarial o amb un ordinador d'escriptori avançat d'ús general, i requereix 1 GB de memòria i 20 GB d'espai en el disc dur. El sistema és extremadament fiable, segur, i es pot utilitzar per proporcionar interfícies virtuals de Windows o Linux. Per obtenir la virtualització basada en el maquinari, el processador haurà de ser de 64 bits i les extensions de virtualització han d'establir-se disponibles i habilitades al processador.

Si efectuem una instal·lació estàndard de CentOS7, el volum 'root' que es crea es molt petit, al voltant de 50GB, i la resta de la grandària del disc la hi assigna al volum

'home'. Això pot ser un inconvenient per a quan es desitja tindre mes espai en la partició root, en concret es parla del moment en que es planifiquen les mides de les imatges de les màquines virtuals. Per tal motiu, cal baixar la grandària del directori /dev/mapper/centos-home i pujar el directori /dev/mapper/centos-root, amb la mida de la memòria necessària de totes les màquines virtuals, en aquest cas es necessita que el directori root tingui almenys 500GB.

7.4 Maquinari virtualitzat

7.4.1 Tallafocs

Per incloure un Tallafocs que proporcioni les característiques per realitzar les comunicacions i l'encaminament entre tots els dispositius de la xarxa local, la zona desmilitaritzada i l'accés a Internet, s'ha seleccionat pfSense, una distribució FreeBSD que inclou gairebé totes les funcionalitats dels costosos firewalls comercials i totes les funcions són administrables amb interfície web, sense l'ajuda de la consola.

PfSense pot instal·lar-se en qualsevol ordinador o servidor que compti amb un mínim de 500 Mhz de velocitat en la seva CPU, 256 MB de memòria RAM, 1 GByte d'emmagatzematge i dues targetes de xarxa, i el procés d'instal·lació és similar a FreeBSD. Encara que la documentació oposada indica que té algunes limitacions, aquest programari ofereix nombroses funcionalitats. pfSense suporta una varietat d'entorns de virtualització de tipus 1 i de tipus 2, com ara VMware, vSphere, Fusion o Workstation, Proxmox, VirtualBox, Xen, KVM, Hyper-V, etc...

Filtrat segons protocols, adreces i ports d'origen i destinació per a trànsit TCP i UDP. Permet crear i visualitzar els registres creats a partir de les regles. Possibilitat de creació d'àlies de grups d'IP i noms d'IP, xarxes i bridges, característiques que ajuden a mantenir la configuració neta i fàcil d'entendre. La taula d'estat del Tallafocs manté informacions de les connexions obertes.

El Port forwarding inclou un rangs i ús d'IP públics múltiple, NAT 1:1 per a IP individuals o subxarxes. Outband NAT, per al tràfic en sortida a l'IP de la WAN, NAT Reflection, per a serveis que poden accedir amb IP públics des de xarxes internes. Balanceig de càrrega en la sortida utilitzat a la xarxa WAN. El tràfic pot ser directe a un gateway designat o a un pool de balanceig de càrrega definit en les regles de base del Tallafocs. Ofereix tres opcions per a la connectivitat VPN, IPsec, OpenVPN i PPTP.

Es visualitza la informació sobre la utilització de la CPU, el trànsit suportat, l'estat del Tallafocs, el trànsit individual de les interfícies, el 'rate' per a totes les interfícies o temps de resposta. Es mostra el trànsit en temps real per a totes les interfícies i en temps real, la càrrega de la CPU, memòria, swap, espai disc utilitzat i la taula d'estat. Client de DNS Dinàmic i portal captiu, que permet de forçar l'autenticació o redirigir el trànsit de xarxa a una pàgina d'autenticació de xarxa. Opcions d'autenticació, usuaris locals i autenticació RADIUS. Inclou DHCP Server i funcionalitat Relay.

The screenshot displays the pfSense web interface. The top navigation bar includes menus for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and FW.reyes.local. The main content area is titled 'Status / Dashboard' and contains several panels:

- System Information:**
 - Name: FW.reyes.local
 - User: creyesrod@172.16.0.254 (Local Database)
 - System: pfSense, Netgate Device ID: 4a95f9e740fb40f1438e
 - BIOS: Vendor: Seabios, Version: 0.5.1, Release Date: Sat Jan 1 2011
 - Version: 2.4.4-RELEASE-p1 (amd64), built on Mon Nov 26 11:40:26 EST 2018, FreeBSD 11.2-RELEASE-p4
 - Update info: Version 2.4.4_3 is available. Version information updated at Tue May 21 20:23:16 UTC 2019
- Interfaces:**
 - WAN: 100baseTX, 192.168.1.200, <full-duplex>
 - LAN: 100baseTX, 172.16.0.1, <full-duplex>
 - OPT1: 100baseTX, 10.0.0.1, <full-duplex>
- Gateways:**

Name	RTT	RTTsd	Loss	Status
GW_WAN 192.168.1.1	0.9ms	0.1ms	0.0%	Online
- Services Status:**

Service	Description	Action
dpinger	Gateway Monitoring Daemon	Refresh/Stop/Start

Figura 14. pfSense

7.4.2 Servidor de Domini

Zentyal és un servidor basat en l'arquitectura GNU/Linux, que permet als professionals administrar els principals serveis de la xarxa local, com ara l'accés a Internet, la compartició de recursos i la infraestructura de la xarxa a través d'una única plataforma i sobre una interfície visual.

Zentyal funciona sobre arquitectures estàndard x86, 32 bits, o x86_64, 64 bits. Per l'àmbit d'una empresa de deu a quinze treballadors seran necessaris com a mínim 1GB de RAM i 250 GB de memòria d'emmagatzematge. Alguns mòduls tenen baixos requeriments, com tallafocs, DHCP o DNS, però altres com el filtrat de correu o l'antivirus necessiten més memòria RAM i CPU.

Zentyal es distribueix en dos paquets: Zentyal Server per a Pimes i Zentyal Cloud per a proveïdors de hosting. Zentyal Server té una edició de desenvolupament que pot descarregar-se de forma gratuïta i el codi està disponible sota els termes de la GNU General Public License. Zentyal és una aplicació web que utilitza el servidor web Apatxe.

El seu disseny incorpora tècniques de programació modernes com:

- Patrons de disseny: un patró de disseny observador usat principalment per a integrar diferents mòduls en Zentyal. Per exemple, cada servei informa sobre que ports necessiten que estiguin oberts. A més, un patró Singleton usat per a emmagatzemar la configuració i comportament global.
- Desacoblament de la lògica i presentació: la interfície d'usuari usa CSS i AJAX, i inclou diversos components Mason, com una taula genèrica usada per a configurar serveis. La lògica del programa resideix en els paquets de les biblioteques.

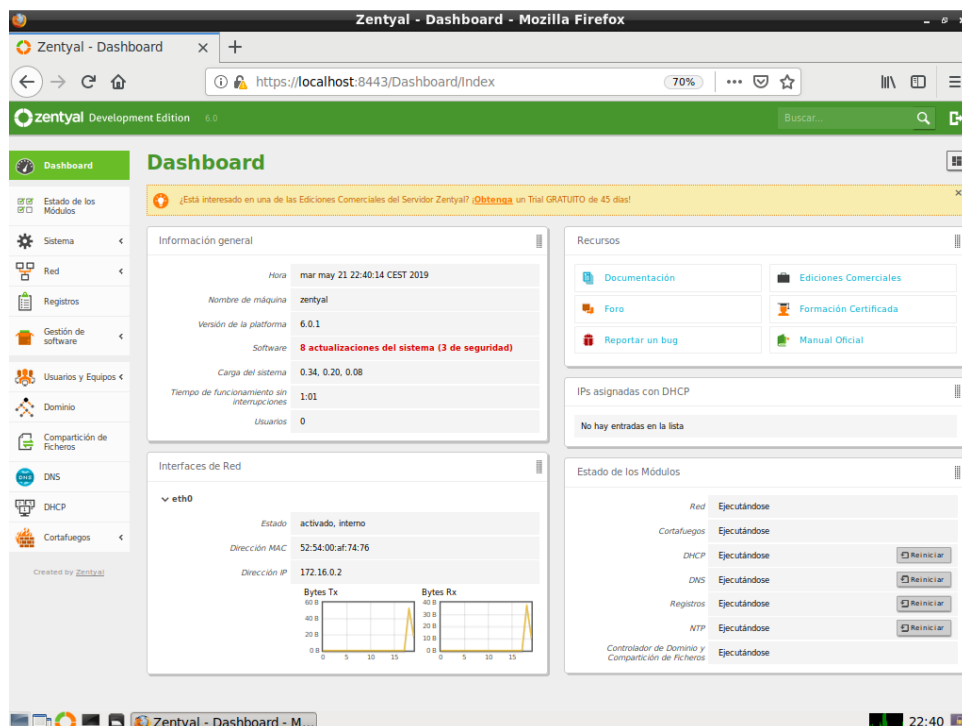


Figura 15. Zentyal Server

Aquestes son les principals característiques que han fet la utilització de Zentyal com servidor de Domini:

- Tolerància a fallides, els errors i avisos es manegen a través d'excepcions programari, anant des del nucli fins a la rutina manejadora.
- Compatibilitat nativa amb els protocols de Microsoft® Exchange Server.
- Suport per a Microsoft Outlook® 2007, 2010.
- Compatibilitat nativa amb Microsoft Activi Directory® 2008, 2008R2, 2012.
- Correu electrònic, calendaris, contactes.
- Sincronització amb dispositius mòbils (suport per a ActiveSync®).
- Antivirus i antispam.
- Empaquetat en un servidor basat en Ubuntu, que inclou controlador de domini i servei de directori, serveis bàsics de xarxes i tallafocs.

7.4.3 Servidor Web y Servidor FTP

Serán las dos distribuciones que substitueixen els actuals servidors WEB i FTP, s'instal·laran dues versions del sistema operatiu CentOS7 però amb les funcionalitats exclusives per oferir aquests dos serveis. La seva ubicació recau a la zona desmilitaritzada de la nostra infraestructura lògica, i d'aquesta forma és mantenen separats de la xarxa local. Aquesta situació evita problemes a l'hora d'executar programes o accedir a determinats serveis des de l'exterior.

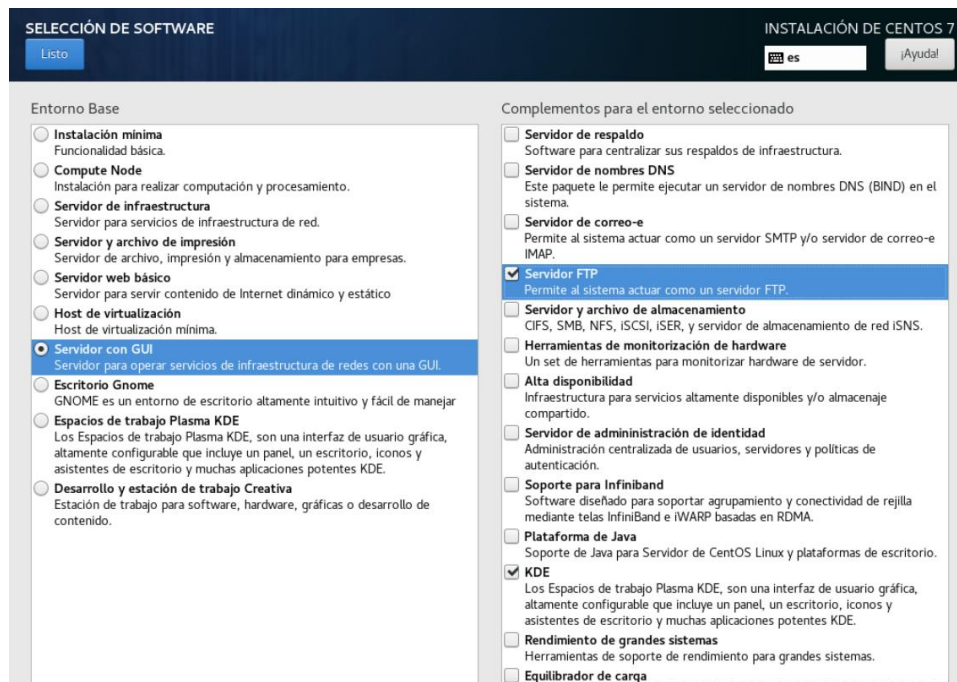


Figura 16. Configuració servidors DMZ

En el cas que quedin oberts tots els ports al Tallafocs, implicaria que qualsevol persona des d'Internet podria realitzar un rastreig per a detectar vulnerabilitats a els serveis que s'estan utilitzant. Això vol dir que el nou servidor WEB i el nou servidor FTP s'han de disposar d'un Tallafocs que limiti la forma d'accés aquest equips. Al nostres cas, és tancaran tots els serveis excepte les comunicacions que és realitzen mitjançant els ports utilitzats per a els protocols 'http', 'https' i 'ftp'.

Depenent de la versió de CentOS7, els requisits de maquinari poden ser molt diferents:

- Des d'una interfície gràfica d'usuari, CentOS funciona amb 512 MB de memòria.
- A la terminal de línia d'ordres només necessita 120 MB,

Adicionalment recomanen 5 GB de memòria, o almenys 1GB. Per controlar-lo en la interfície de línia d'ordres, que ja no està inclosa com a opció independent en CentOS 7. Per defecte, aquesta distribució de Linux utilitza 1 GB de RAM i 20 GB, o almenys 10 GB, d'espai en disc dur.

7.5 Servidor de vitalització.

A fi de triar un servidor es necessita saber exactament quantes i quins tipus d'aplicacions s'executen, i la quantitat d'usuaris que es connectaran. El temps de funcionament també és un factor crític, mentre més depengui l'empresa del servidor per a realitzar les seves funcions quotidianes, més robust i potent haurà de ser el servidor. No s'ha de pensar tan sols en termes de maquinari, sinó també en termes del programari que s'executarà. S'ha de conèixer les necessitats de CentOS7, el sistema operatiu que convertirà el maquinari en un servidor de virtualització i els requisits de les màquines virtuals que s'allotgen en ell.

	RAM(GB)	Disc (GB)	Arquitectura
CentOS7 KVM (S.O)	1	50	x86_64
pFSense	0,128	15	amd_64 or Intel 64 bits CPU
Zentyal	1	250	x86_64
CentOS7 Web	1	35	x86_64
CentOS7 FTP	1	150	x86_65
Totals	4,128	500	

Taula 1. Requisits mínims de memòria per al Servidor de Virtualització

En aquesta infraestructura conviurà el programari propietari per algunes de les estacions de treball actuals, i el nou programari lliure utilitzat en la construcció del nou servidor de virtualització. No volem emmarcar la solució únicament en la utilització de programari lliure, i es preveu la possibilitat que en un futur sigui necessari adherir-se a una plataforma de programari propietari. Per aquests motius utilitzarem un processador de 64 bits amb 6 cores, 16GB memòria RAM i 2TB de disc dur⁷.

Hauem d'utilitzar un servidor de virtualització enrackable per a situar-lo en el nou armari de comunicacions, aquesta configuració usa l'espai de manera eficient i ofereix una gestió centralitzada del cablejat. A més, la configuració d'un servidor Rack augmenta l'escalabilitat de la infraestructura, ja que possibilita afegir nous servidors segons sigui necessari.

El servidor enrackable ofereix màxim poder computacional amb un disseny intel·ligent pel que fa a l'aprofitament de l'espai i flexibilitat per a barrejar i combinar aplicacions i càrregues de treball. És un model que té ranures d'expansió, conegudes com a ranures 'mezzanine', per a afegir targetes d'interfície de xarxa, entre altres coses. Els ventiladors poden fer molt de soroll, i l'empresa també haurà de tenir un sistema de control climàtic per a mantenir el Rack a la temperatura ideal. Per això, cal aïllar els servidors Rack en una sala especial.

El servidor de virtualització permet una utilització més eficient dels recursos, col·loca una capa d'abstracció entre el sistema operatiu i el maquinari, pot operar amb

⁷ Vegeu annex 13.3: Especificacions, DELL Power Edge R340 enrackable, p. 70.

diverses màquines amb i diferents sistemes operatius en el mateix servidor físic. Per això la major part del temps estan per sota del seu òptim rendiment. Una empresa pot utilitzar aquests recursos de forma més eficient, ja que elevarà entre un 60 i 80% el nivell d'utilització dels servidors.

7.6 NAS, Network Attached Storage

L'emmagatzematge connectat en xarxa, Network Attached Storage, és una tecnologia d'emmagatzematge dedicada a compartir la capacitat d'un servidor amb computadors personals o servidors clients a través d'una xarxa. Aquest element físic s'utilitzarà per a albergar les còpies de seguretat de tots els arxius, documents i bases de dades. Els protocols de comunicacions NAS estan orientats a manipular una gran quantitat de petits arxius. Els protocols usats són protocols de compartició d'arxius com Network File System, NFS o Microsoft Common Internet File System, CIFS.

Un servidor NAS disposa de CPU, memòria RAM i un sistema operatiu, normalment un basat en Linux. Un model amb 512MB de RAM i un processador Dual Core és més que suficient, però aquesta infraestructura, buscarem un NAS almenys de 2 GB i una CPU de quatre nuclis, com utilitzarem el dispositiu per gestionar arxius de diferents usuaris, millor utilitzar un aparell amb bones capacitats.

Cal triar un bon disc dur i cal considerar seriosament la seva capacitat d'emmagatzematge i quin tipus de discos durs es fan servir en ells. Normalment els NAS es venen sense discos durs i cal adquirir els més adequats. Els servidors NAS més senzills només tenen un buit per a un disc dur, però segons anem pujant de nivell, podrem anar incorporant més i més discos durs. Des 1TB/2TB els més simples, passant per 6TB/8TB per a guardar fitxers, fins a 10TB/20TB perfectes per a oficines. En aquest cas, es precis almenys un servidor NAS amb quatre badies amb dos dispositius d'emmagatzematge de 10TB de capacitat total. Sovint, aquests dispositius estan disposats en RAID, Redundant Arrays of Independent Disks o contenidors d'emmagatzematge redundants⁸.

7.7 Xarxa virtual per l'Hipervisor.

Un cop triat l'Hipervisor tipus 2, KVM, allotjat en el Sistema operatiu CentOS7, i el tipus de maquinari a virtualitzar, en aquest apartat s'exposen els diferents serveis i programari que permeten crear les xarxes on es connectaran les màquines virtuals i l'entorn físic de la infraestructura. En el moment de realitzar el estudi per realitzar l'escenari de proves del projecte, es va realitzar la connectivitat a través de les xarxes creades directament amb KVM/Qemu i no es va aconseguir el resultat esperat. En el moment de crear les diferents xarxes s'apreciava que el servidor de virtualització no

⁸ Vegeu annex 13.4: Especificacions, Synology NAS, p. 71.

funcionava correctament, algunes de les seves funcions deixaven de comportar-se amb normalitat.

Es desestima el concepte de la instal·lació d'una targeta de xarxa per a cadascuna de les màquines virtuals que s'executen, ja que per exemple, amb la proposta es poden configurar enllaços troncal cap a la interfície física i connectar-la a un commutador físic que sigui capaç de separar o treballar amb les diferents xarxes virtuals. Aquest nou concepte pot estalviar despeses en la adquisició de diferents interfícies físiques per ubicar al maquinari i treure futurs punts de fallides.

La virtualització de xarxa, mitjançant el commutador virtual Open Virtual Switch operant dins l'Hipervisor, permet crear totes les xarxes necessàries i comunicar amb garanties les diferents màquines virtuals ubicades en diferents xarxes i amb els elements del entorn físic. La unió dels servei de xarxa network.service i la IP suite que opera dins de CentOS, juntament amb el programari Open Virtual Switch permetrà crear les xarxes necessàries dins l'Hipervisor.

7.7.1 Network Service

El servei 'network' activa o desactiva totes les interfícies de xarxa configurades per iniciar-se en el moment d'arrencar. La xarxa tradicional TCP/IP v4 sempre està habilitada si es fa servir la xarxa. El nou TCP/IP v6 pot habilitar selectivament aquí.

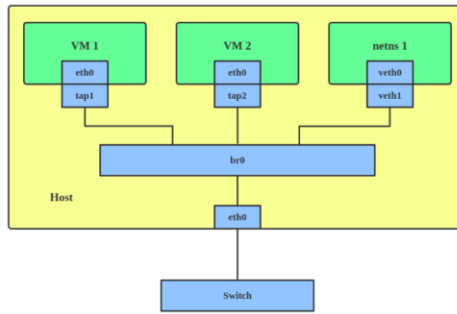
A CentOS7 les interfícies de xarxa individuals, sovint anomenades 'nic', tenen un arxiu de configuració en el directori /etc/sysconfig/network-scripts. Per convenció, cada arxiu de configuració de la interfície de xarxa es diu ifcfg-[nom] i es localitza mitjançant una recerca ifcfg-* de patró de comodí. El contingut d'un arxiu de configuració nic varia segons el tipus d'interfície i la xarxa.

7.7.2 suite 'iproute2'

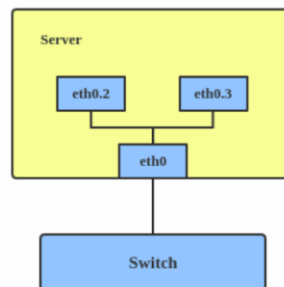
Com a part de la suite iproute2, les comandes 'ip link' ofereixen la capacitat de mostrar informació de la capa d'enllaç, activar una interfície, desactivar una interfície, canviar les banderes d'estat de la capa d'enllaç, canviar la MTU, el nom de la interfície i fins i tot la direcció de transmissió Ethernet i maquinari.

Aquests són els objectes utilitzats per proporcionar la connectivitat a les interfícies de les màquines virtuals:

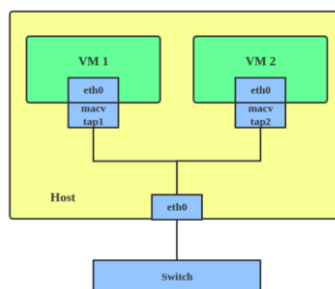
- **Bridge:** Un pont de Linux es comporta com un commutador de xarxa. Reenvia paquets entre les interrelacions que estan connectades a ell, normalment es fa servir per reenviar paquets a encaminadors, portes d'enllaç o entre màquines virtuals i dominis de xarxa en un mateix host. Utilitzem un pont quan volem establir canals de comunicació entre màquines virtuals, contenidors i els seus hosts.

Figura 17. Bridge⁹

- **Vlan:** Separa les màquines virtuals agregant etiquetes als paquets de xarxa. Permeten als administradors de xarxa agrupar els hosts en el mateix commutador o entre commutadors diferents. S'utilitza una Vlan quan es vol separar subxarxes en màquines virtuals, dominis o hosts.

Figura 18. Vlan¹⁰

- **Macvtap / Ipvttap:** Es un nou controlador de dispositiu destinat a simplificar les xarxes pontades virtualitzades. Quan es crea una instància de Macvtap/Ipvttap a la part superior d'una interfície física, el nucli també crea un dispositiu per ser utilitzat com un dispositiu utilitzat directament per KVM/qemu. En general, Macvlan/Ipvlan s'utilitza perquè tant el convidat com el host es mostrin directament en el commutador al qual està connectat el host.

Figura 19. Macvtap¹¹

⁹ Enllaç Figura 17: <https://developers.redhat.com/blog/wp-content/uploads/2018/10/bridge.png>

¹⁰ Enllaç Figura 18: <https://developers.redhat.com/blog/wp-content/uploads/2018/10/vlan.png>

¹¹ Enllaç Figura 19: <https://developers.redhat.com/blog/wp-content/uploads/2018/10/macvtap.png>

7.7.3 Open Virtual Switch

Open vSwitch, abreujat OVS, és un programari de codi obert, dissenyat per ser utilitzat com un commutador virtual en entorns de servidors virtualitzats. És l'encarregat de tornar a enviar el trànsit entre diferents màquines virtuals en el mateix host físic, i entre les màquines virtuals i la xarxa física. Sota la llicència Apache 2.0.

Open vSwitch és un programari multicapa per commutadors, l'objectiu és la implementació d'una plataforma de qualitat que suporti interfícies de gestió estàndard i exposi les funcions de forwarding de forma programable. Podem dir, que Open vSwitch és una de les implementacions més populars de OpenFlow.

Està ben adaptat per funcionar com un commutador virtual en ambients implementats amb màquines virtuals. A més d'exposar interfícies estàndard de control i visibilitat amb la capa de xarxa virtual, va ser dissenyat per suportar una distribució a través de múltiples servidors físics. La major part del codi està escrit sobre una plataforma independent a C i és fàcilment portable a altres entorns. La versió actual d'Open vSwitch és compatible amb les següents característiques:

- Model estàndard de **Vlan 802.1q** amb ports troncal i d'accés.
- NetFlow i sFlow: possibilitat de treure paquets del protocol **NetFlow** que serveixen per capturar informació sobre el trànsit IP, i sFlow, paquets del protocol **sFlow** dissenyat per monitorització d'interfícies, dispositius wireless i de l'equip amfitrió, entre màquines virtuals, que poden ser capturats i analitzats.
- OpenFlow 1.0 o extensions posteriors.
- **SPAN**, commutador port Analyzer, i **RSPAN**, Remote SPAN: Ens permet fer mirroring d'un port o fins i tot d'un bridge sencer, és a dir, enviar una còpia dels paquets vistos en un port del commutador, o Vlan sencera, a una connexió per al monitoratge de xarxa en un port del commutador i d'aquesta manera poder dur a terme el diagnòstic d'errors a la xarxa.
- **LACP**, Bonding, IEE 802.1 Ax-2008: permet balancejar el trànsit entre diversos enllaços, LACP és a nivell de commutador exterior, trunking, i el bonding a nivell de màquina virtual.
- **STP**, Spanning Tree Protocol, IEEE 802.1d-1998: és un protocol de xarxa de nivell 2 del model OSI. La seva funció és la gestió de bucles en topologies de xarxa.
- Polítiques de trànsit per port, **firewalling**.
- **QoS**: Serveix per definir els nivells de qualitat de servei com disponibilitat, ample de banda, ràtio d'error, latència, prioritzar trànsit, etc.
- **Protocols de túnel Múltiples**, GRE, VXLAN, IPsec, GRE i VXLAN sobre IPsec.
- Suport per Bidirectional Forwarding Detection, **BFD**.
- Suport per **HFSC qdisc**: és un algoritme que permet prioritzar el trànsit en una xarxa basant-se en QoS, qualitat de servei, i CBQ, Class-based queuing o deixar a la cua basat sobre classes, shaping.
- Selecció d'eines per al monitoratge d'enllaços 802.1ag, **CFM**, estàndard per a xarxes de ponts virtuals i metropolitanes, que defineix una sèrie de protocols i pràctiques per a operacions, administració i manteniment per ponts i xarxes locals.

Open vSwitch Disposa d'un disseny de major complexitat que els 'bridges', mentre que a els bridges només s'executen a l'espai del nucli del host, l'Open vSwitch, codifica amb més complexitat que a els 'bridges' i permeten proporcionar totes els funcionalitats avançades, a banda de fer ús de l'espai del nucli, també s'executa en el espai de l'usuari.

Sabem que el espai del nucli i el espai de l'usuari són dos separacions lògiques de la memòria dels Sistemes Operatius, i així es pot protegir al sistema de fallades o atacs. A l'espai del nucli s'executen els mòduls i els controladors del sistema, mentre que a l'espai d'usuaris és trobaria la majoria del programari.

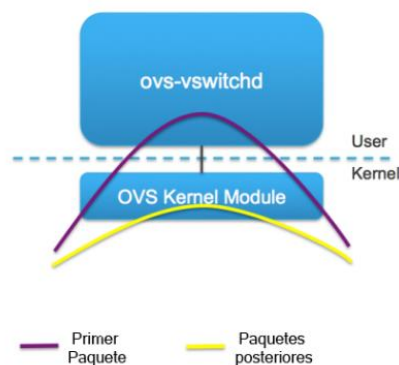


Figura 20. Procés d'intercanvi de OVS¹²

Principals components

- **OVS-vswitchd**: És un dimoni que implementa les funcionalitats del commutador, juntament amb el mòdul del nucli `openvswitch_mod.ko`, un mòdul del nucli de Linux per commutació basada en fluxos. Aquest procés és el Core de l'Open vSwitch, s'ha de comunicar amb els altres dos components.

El procés 'OVS-vswitchd' ha de comunicar-se amb el 'ovsdb-server' per poder guardar i aplicar les configuracions emmagatzemades a la base de dades albergada pel servidor 'ovsdb-server'. Aquesta comunicació es realitza mitjançant sockets Unix amb el protocol OVSDDB. El mòdul del nucli `openvswitch_mod.ko` també ha de ser contactat pel dimoni OVS-vswitchd per poder prendre decisions sobre els nous fluxos que proporciona el nucli. Utilitza el protocol Netlink el qual permet comunicar l'espai del nucli amb el de l'usuari.

- **Ovsdb-server**: És un servidor de base de dades lleuger que 'OVS-vswitchd' consulta per obtenir la seva configuració. A la base de dades que gestiona es troben tots els paràmetres de configuració de l'Open vSwitch, els quals s'emmagatzemen de manera que aquesta informació es manté després d'un reinici de l'ordinador central.

¹² Enllaç figura 20: https://es.wikipedia.org/wiki/Open_vSwitch#/media/Archivo:Openvswitch.jpg

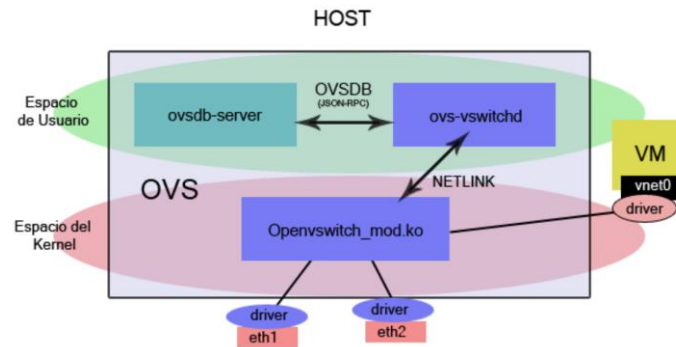


Figura 21. Principals components de OVS¹³

Algunes de les taules que hi ha en aquesta base de dades, les quals contenen la configuració dels seus elements corresponents són:

- **Open_vSwitch**, la configuració de l'Open vSwitch.
- **Bridge**, la configuració dels bridges.
- **Port**, la configuració dels Ports.
- **Interface**, la configuració dels dispositius físics de xarxa.
- **Flow_Table**, la configuració de la taula OpenFlow.
- **QoS**, la configuració de la Qualitat de Servei.
- **Queue**, la configuració de cues.
- **Mirror**, la configuració de la interfície mirall.
- **Controller**, la configuració del controlador OpenFlow.
- **Manager**, la connexió a l'administració d'OVSDB.
- **NetFlow**, la configuració de NetFlow.
- **SSL**, la configuració de SSLs.
- **sFlow**, la configuració de sFlow.

Aquesta base de dades pot ser modificada des elements externs utilitzant el protocol Open vSwitch Database Management Protocol, OVSDB.

- El mòdul del nucli **openvswitch_mod.ko** és qui maneja el 'packet switching'. No pot ser modificat mitjançant Openflow, ni dur a terme l'esborrat de fluxos, tan sols fa servir una memòria cau en la qual li diu que ha de fer amb cada flux.
- **OVS-brcompatd**: un dimoni que permet OVS-vswitchd actuar com un reemplaçament momentani del bridge de Linux.
- **OVS-dpctl**: eina per a configurar el mòdul del nucli del commutador.
- **OVS-appctl**: és una utilitat que envia ordres per executar els dimonis d'Open vSwitch.
- **OVS-vsctl**: és una utilitat per a consultar i actualitzar la configuració del OVS-vswitchd.
- **OVS-ofctl**: per mostrar els fluxos escorcollats.
- **Ovsdbmonitor**: és una eina de GUI per a la visualització remota de les bases de dades OVS i les taules de flux OpenFlow.

¹³ Enllaç figura 21: https://es.wikipedia.org/wiki/Open_vSwitch#/media/Archivo:OVS_sin_Controller.jpg

Open vSwitch pot ser portat a diferents plataformes de maquinari i diferents sistemes operatius. A més s'executa en servidors físics i suporta l'administració remota d'una manera que fa que sigui més fàcil per els desenvolupadors de les plataformes de virtualització. La configuració de l'Open vSwitch és controlada per un esquema de base de dades organitzada en diferents taules, tot realitzat a l'espai d'usuari ja que el mòdul del nucli s'utilitza estrictament per a la transmissió. Aquesta base de dades és persistent a els reinicis, i està basat en JSON.

Avantatges del OVS

Sabem que Open vSwitch és un substitut dels bridges a l'hora de donar connectivitat a les màquines virtuals. A més, que el seu funcionament pugui ser a través d'un 'controller' o 'standlone' dona certes avantatges, mentre que altres són exclusius de la utilització de fluxos programats regits únicament pel controlador.

Incorporen funcionalitats de xarxa similars als commutadors de maquinari, a banda de les funcionalitats L2 i L3, Vlan etiquetades, per port, i afegir enllaços. Del mateix mode administra funcionalitats pròpies d'un commutador de maquinari configurable, que són les que característiques compatibles que definíem anteriorment com poden ser SPAN/RSPAN, NetFlow/sFlow, QoS, Túnel GRE, etc...

Les configuracions de Vlans i 'agregats' es realitzen directament sobre l'Open vSwitch, no sobre tercers elements com poden ser 'bondings', un bridge per Vlan, etc... La compatibilitat amb programari basat en bridges s'hauria de configurar de manera que imités el comportament d'un 'bridge' enfront de les Vlans, tindríem un 'bridge' per cada Vlan en lloc de tenir un Open vSwitch, en el qual es necessita, per cada port, una configuració pròpia com si fos un commutador tradicional.

El processament de paquets a maquinari es un avantatge afegit d'Open vSwitch que permet realitzar un 'offloading' del processament de paquets a les nics dels hosts de KVM, en els quals resideixen, en lloc de fer-ho per Software, amb la qual cosa així es millora del rendiment.

Xarxes privades virtuals: Un creixent segment de la virtualització és el 'cloud hosting', en el qual, un host aliè acull les màquines virtuals de múltiples clients o convidats. Ideat per utilitzar millor el maquinari, aquests ambients han de co-localitzar als inquilins a la mateixa infraestructura física i proporcionar fortes garanties d'aïllament al mateix temps.

De la mateixa manera que un grup de màquines físiques poden estar connectades entre si a través d'una xarxa dedicada, en un entorn virtualitzat una col·lecció de màquines virtuals poden estar connectades entre si a través d'una xarxa privada virtual implementada a la part superior d'una infraestructura de xarxa física compartida.

Si totes les màquines virtuals d'un sol arrendatari estan al mateix host físic, o si estan en hosts separats on cadascú dedica una nic per connectar-ne a un commutador físic aïllat, el suport a aquestes xarxes privades virtuals és simple.

No obstant això, quan les màquines virtuals que comparteixen una xarxa privada és distribueixen en diversos hosts i commutadors físics, la capa de xarxa de virtualització ha de suportar la creació dinàmica de superposició. Open vSwitch suporta túnels de tipus GRE i Vlan.

Mobilitat entre Subxarxes: una limitació per les plataformes de virtualització comercials és que la migració ha de passar dins d'una mateixa subxarxa IP. Això es deu a la impossibilitat de mantenir sessions de transport 'Tcp' si es canvia la direcció del host destinació. Si una xarxa té problemes d'escalament pel que fa al nombre de hosts, hi ha diverses formes d'aconseguir això amb Open vSwitch.

La més directa és unir un model similar al mòbil IP, en el qual un Open vSwitch base rep tots els paquets dirigits a una màquina virtual i després els torna a enviar a la veritable direcció del host. El procés de gestió global ha de gestionar les tunelitzacions consistents en la localització de les màquines virtuals dins de la xarxa.

8 Implementació

8.1 Instal·lació del sistema operatiu

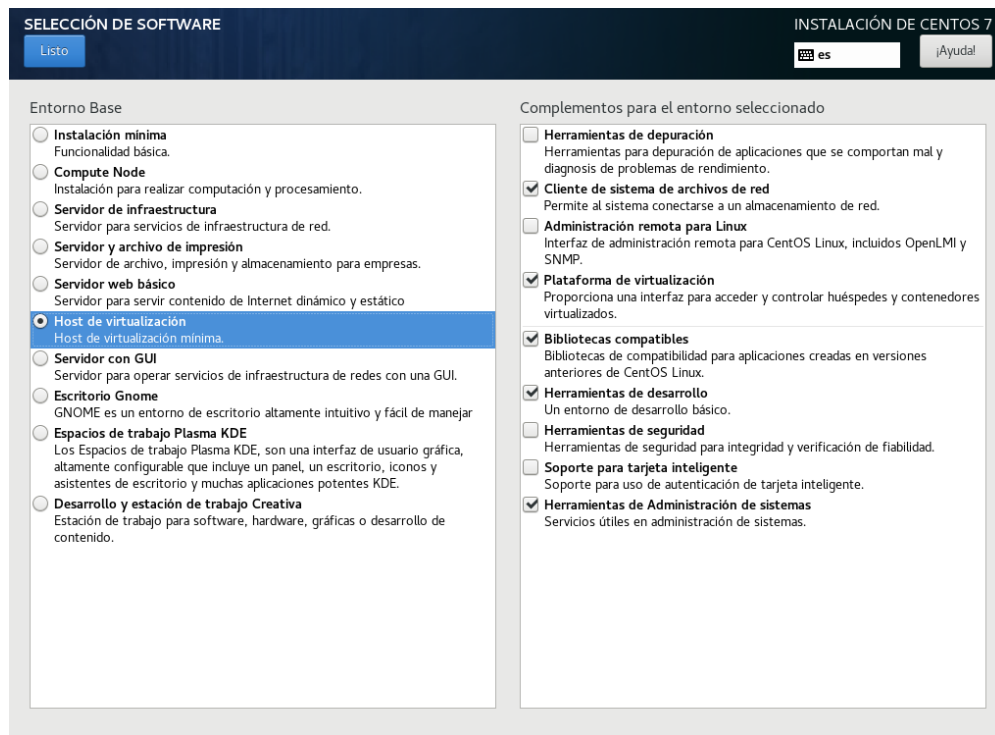


Figura 22. Screenshot Instal·lació de CentOS7

La versió inicial instal·lada únicament es comandarà mitjançant el terminal o 'shell', per aquest motiu es necessari incloure GNOME per operar amb les màquines virtuals i realitzar diferents operacions en la gestió del servidor. Una vegada acabada la instal·lació principal es permet la instal·lació de GNOME, i serà necessari reiniciar el servidor.

```
su
```

```
yum install group "GNOME Desktop" "Graphical Administration Tools"
ln -sf /lib/systemd/system/runlevel5.target /lib/systemd/system/default.target
reboot
```

8.2 Instal·lació de KVM

En primer lloc, és necessari conèixer l'estat i el tipus de virtualització de la 'cpu'.

```
grep -o vmx /proc/cpuinfo
lscpu | grep Virtualization
```


Instal·lació dels paquets libvirt, qemu i el gestor de les màquines virtuals.

```
su
yum install qemu-kvm virt-install virt-manager virt-viewer libguestfs-tools libvirt*

lsmod | grep -i kvm
ps -ef | grep libvirtd
```

Activació del servei.

```
systemctl enable libvirtd.service
systemctl start libvirtd.service
systemctl status libvirtd.service
chkconfig libvirtd on
```

8.3 Instal·lació de Open VSwitch

És el moment de seleccionar una de les diferents tecnologies que permetrà crear les xarxes que connecten les màquines virtuals, la intenció es recrear qualsevol escenari possible, lògicament dins de les possibilitats que ens ofereix el maquinari i programari amfitrió. L'opció triada per aquest treball es Open Virtual commutador en lloc dels components de xarxa que la suite iproute2 ofereix a KVM. La combinació entre OVS i 'libvirt' instal·lada a Centos7 ofereix una estabilitat més gran i una notable comunicació entre l'amfitrió i el convidat.

OVS és fonamental per a moltes implementacions en centres de dades, ja que uneix les màquines virtuals dins d'una instància d'Hipervisor en un servidor, és el primer punt d'entrada per totes les màquines virtuals que inclouen trànsit a la xarxa. Totes les funcionalitats que s'estableixen a OVS són necessàries per simplificar els requisits per abastir al Hipervisor de totes les funcionalitats per a crear qualsevol escenari.

Amb el sistema de repositoris i l'eina de gestió de paquets de Centos7 es descarrega el software per treballar amb Open Virtual Switch.

```
su
yum install wget openssl-devel python-sphinx gcc make python-devel openssl-devel kernel-devel graphviz kernel-debug-devel
autoconf automake rpm-build redhat-rpm-config libtool python-twisted-core python-zope-interface PyQt4 desktop-file-utils
libcap-ng-devel groff checkpolicy selinux-policy-devel -y
```

Posteriorment es descarrega Open VSwitch versió 2.9, és necessari crear un usuari ovs per a realitzar la instal·lació.

```
useradd ovs
su - ovs

mkdir -p ~/rpmbuild/SOURCES
wget http://openvswitch.org/releases/openvswitch-2.9.2.tar.gz
cp openvswitch-2.9.2.tar.gz ~/rpmbuild/SOURCES/
tar xzf openvswitch-2.9.2.tar.gz
rpmbuild -bb --nocheck openvswitch-2.9.2/rhel/openvswitch-fedora.spec
exit
```

Una vegada fora la sessió del usuari ovs, es podrà iniciar la instal·lació.

```
yum localinstall /home/ovs/rpmbuild/RPMS/x86_64/openvswitch-2.9.2-1.el7.x86_64.rpm -y
```

Activació del servei.

```
systemctl start openvswitch.service
systemctl enable openvswitch.service
systemctl status openvswitch.service
ovs-vsctl -V
```

8.4 Preparació de les xarxes virtuals

Per a poder realitzar l'escenari proposat serà adient implementar tres xarxes diferents:

- la xarxa WAN, que serà la que ens proporcioni la sortida cap a l'exterior o Internet.
- la xarxa LAN, per a albergar els dispositius de la xarxa local tant físics com virtuals.
- la xarxa desmilitaritzada o DMZ, per a situar màquines virtuals on l'accés es pot fer des de Internet.

En primer lloc, inserirem un Tallafocs per a governar i proporcionar la comunicació entre les diferents xarxes en l'escenari suggerit. Serà el gestor d'oferir encaminament i polítiques de seguretat entre les diferents xarxes. El Tallafocs serà l'encarregat de proporcionar la connectivitat, la seguretat i els permisos entre les diferents xarxes.

La connectivitat de les màquines virtuals i els dispositius de xarxa físics es faran a través de tres xarxes virtuals diferents. La comunicació del servidor de virtualització amb l'exterior, es realitzarà a través del commutador que proporciona l'encaminador per a la connectivitat interna, encara que es podria realitzar a través d'interfícies identificades mitjançant direccions públiques. Disposarem de control total de la màquina virtual i podrem accedir des de qualsevol dispositiu connectat dins de la xarxa local, ja sigui virtual o física.

La xarxa privada amb accés a l'exterior serà la 192.168.1.0/24. Aquesta xarxa utilitzarà un ovs-bridge, que denominarem 'ovs-br-wan' per a proporcionar al Hipervisor i a l'escenari virtual la sortida cap a Internet amb connectivitat a través d'una interfície física del nostre servidor.

La xarxa local obtindrà mitjançant la interfície virtual LAN del Tallafocs la possibilitat de comunicar-se amb les diferents xarxes i proporcionar la sortida cap a Internet. En

aquest cas la xarxa local serà la 172.16.0.0/24 i utilitzarà un ovs-bridge, que denominarem 'ovs-br-lan' oferint la connectivitat entre els diferents elements de la xarxa local, ja siguin màquines virtuals o dispositius de xarxa físics.

La zona desmilitaritzada obtindrà mitjançant la interfície virtual DMZ del Tallafocs la possibilitat de comunicar-se amb les diferents xarxes i proporcionar la comunicació amb Internet. En aquest cas la xarxa serà la 10.0.0.0/24, i utilitzarà un ovs-bridge, que denominarem 'ovs-br-dmz' concedint la connectivitat entre l'exterior i el servidor ofert per l'accés extern. Amb el Tallafocs podrem filtrar el tràfic, per exemple, aïllant la zona desmilitaritzada de la xarxa local.

Es configura un bridge mitjançant Open Virtual commutador per a cada xarxa, amb l'objectiu de tenir un punt de connexió on connectar qualsevol dispositiu, ja sigui físic o virtual i serviran per crear les xarxes que utilitzaran les màquines virtuals. Per a realitzar aquest pas es indispensable desactivar el Network Manager que ve per defecte amb GNOME de Centos7:

```
nmcli device status
systemctl stop NetworkManager
systemctl disable NetworkManager
systemctl list-unit-files | grep NetworkManager
```

S'haurà de comprovar si el servei network.manager romandre actiu.

```
systemctl status network.service
```

Creació del bridge-ovs per la xarxa **WAN**, assignació de la direcció, i activació mitjançant la comanda d'ip link.

```
ovs-vsctl add-br ovs-br-wan
ip addr add 192.168.1.254/24 dev ovs-br-wan
ip link set dev ovs-br-wan up
```

Cal fer-ho persistent, es crea un nou arxiu de configuració per ovs-br-wan¹⁴.

Creació del bridge-ovs per la xarxa **LAN**, assignació de la direcció, i activació mitjançant la comanda d'ip link.

```
ovs-vsctl add-br ovs-br-lan
ip addr add 172.16.0.254/24 dev ovs-br-lan
ip link set dev ovs-br-lan up
```

Cal fer-ho persistent, es crea un nou arxiu de configuració per ovs-br-lan¹⁵.

Creació del bridge-ovs per la xarxa **DMZ**, assignació de la direcció, i activació mitjançant la comanda d'ip link.

¹⁴ Vegeu annex 13.1: Arxius de configuració de les interfícies virtuals, p. 68.

¹⁵ Vegeu annex 13.1: Arxius de configuració de les interfícies virtuals, p. 68.

```
ovs-vsctl add-br ovs-br-dmz
ip addr add 10.0.0.254/24 dev ovs-br-dmz
ip link set dev ovs-br-dmz up
```

Cal fer-ho persistent, es crea un nou arxiu de configuració per ovs-br-dmz¹⁶.

Un cop hi son configurats els bridges generats per Open Virtual commutador, un per a cada xarxa, s'afegeixen les interfícies físiques per oferir connectivitat amb elements físics. Seran necessàries dos 'nics', una per la xarxa WAN i un altre per a la xarxa local, la zona desmilitaritzada es connectarà mitjançant una xarxa interna, no tindrà connectivitat amb elements físics, si no que es connectaran únicament màquines virtuals, això si, mantenint la connectivitat amb qualsevol dispositiu en cas que fos necessari.

Adhesió de la interfície física en el bridge de la WAN per a la sortida a Internet, en aquest cas 'eno1', s'ha de buidar l'adreça de la interfície física i afegir-la a 'ovs-br-wan', aquesta interfície ja estava activada i no fa falta aixecar-la, en aquests cas també serà l' interfície del sistema operatiu.

```
ip addr flush dev eno1
ovs-vsctl add-port ovs-br-wan eno1
```

Cal fer-ho persistent, editant l'arxiu de configuració per 'eno1'¹⁷, portarà la direcció MAC del Hardware de la interfície física.

Reinici del servei de xarxa per obtenir els canvis soferts a la configuració.

```
systemctl restart network.service
```

Adhesió de la interfície física en el bridge de la LAN per la connectivitat amb elements físics de una xarxa local, com per exemple un commutador, en aquest cas 'enp2s0', s'ha de buidar l'adreça de la interfície física, afegir-la a 'ovs-br-wan' i activar-la mitjançant la comanda d'ip link, en aquest cas la interfície no estava prèviament activada com 'eno1', que és la que donava connectivitat al programari.

```
ip addr flush dev enp2s0
ovs-vsctl add-port ovs-br-lan enp2s0
ip link set dev enp2s0 up
```

Cal fer-ho persistent, editant l'arxiu de configuració per 'enp2s0'¹⁸, portarà la direcció MAC del Hardware de la interfície física.

Es torna a reiniciar el servei de xarxa per obtenir els canvis soferts a la configuració.

¹⁶ Vegeu annex 13.1: Arxius de configuració de les interfícies virtuals, p. 68.

¹⁷ Vegeu annex 13.2: Arxius de configuració de les interfícies físiques, p. 69.

¹⁸ Vegeu annex 13.2: Arxius de configuració de les interfícies físiques, p. 69.

```
systemctl restart network.service
```

Es configura perquè la ruta per defecte es realitzi a través de la interfície 'eno1', interfície WAN física, mitjançant el arxius de configuració indicat excepte a 'ifcfg-eno1' el paràmetre DEFROUTE="no". Per altre banda, editant l'arxiu de configuració es desactiva ipv6 en les interfícies tant virtuals com físiques, ja que en el nostre cas, la xarxa únicament utilitza direccions ipv4.

```
nano /etc/sysctl.conf

net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1

net.ipv6.conf.eno1.disable_ipv6 = 1
net.ipv6.conf.enp2s0.disable_ipv6 = 1

net.ipv6.conf.ovs-br-wan.disable_ipv6 = 1
net.ipv6.conf.ovs-br-lan.disable_ipv6 = 1
net.ipv6.conf.ovs-br-dmz.disable_ipv6 = 1
```

Per a preservar els canvis.

```
sysctl -p
systemctl restart network.service
```

Libvirt és un joc d'eines C per interactuar amb les capacitats de virtualització de versions recents de Linux i altres sistemes operatius. El programa 'virsh' és la interfície principal per gestionar les màquines virtuals tant a KVM com a altres Hipervisors. El programa es pot utilitzar per crear i aturar els convidats, també es pot utilitzar per conèixer l'estat de les màquines virtuals instal·lades.

Una cop creada l'estructura mitjançant els 'ovs-br' i les connexions a les interfícies físiques s'han d'establir les tres xarxes assignades a cadascun dels ovs-bridges mitjançant 'KVM/virsh'. Es podran configurar les 'nics' de les màquines virtuals a través d'aquestes xarxes en lloc de les interfícies derivades del 'bridges', com per exemple 'macvtap'. Aquest procés proporciona un millor rendiment i en cas que fos necessari s'obtindria connectivitat entre els convidats i l'amfitrió.

Creació de la xarxa WAN.

```
nano /tmp/ovs-network-wan.xml

<network>
<name>ovs-network-wan</name>
<forward mode='bridge'/>
<bridge name='ovs-br-wan'/>
<virtualport type='openvswitch'/>
</network>
```

```
virsh net-define /tmp/ovs-network-wan.xml
virsh net-start ovs-network-wan
virsh net-autostart ovs-network-wan
```

Creació de la xarxa LAN.

```
nano /tmp/ovs-network-lan.xml

<network>
<name>ovs-network-lan</name>
<forward mode='bridge'/>
<bridge name='ovs-br-lan'/>
<virtualport type='openvswitch'/>
</network>
```

```
virsh net-define /tmp/ovs-network-lan.xml
virsh net-start ovs-network-lan
virsh net-autostart ovs-network-lan
```

Creació de la xarxa DMZ.

```
nano /tmp/ovs-network-dmz.xml

<network>
<name>ovs-network-dmz</name>
<forward mode='bridge'/>
<bridge name='ovs-br-dmz'/>
<virtualport type='openvswitch'/>
</network>
```

```
virsh net-define /tmp/ovs-network-dmz.xml
virsh net-start ovs-network-dmz
virsh net-autostart ovs-network-dmz
```

Reinici del serveis per aplicar els canvis.

```
systemctl restart openvswitch.service
systemctl restart libvirtd.service
systemctl restart network.service
systemctl status openvswitch.service
systemctl status libvirtd.service
systemctl status network.service
ovs-vsctl show
virsh net-list
```

8.5 Creació de les màquines virtuals

En l'actualitat, KVM/Qemu suporta diferents formats com raw, cloop, cow, qcow, qcow2, vmdk, vdi per donar-li forma als discos de les seves màquines virtuals, encara que per defecte es fa per amb 'qcow2'. 'qcow' és un format d'arxiu per als la imatge de

disc utilitzats pel monitor de màquina virtual allotjada. Utilitza una estratègia d'optimització d'emmagatzematge en disc que retarda la seva assignació fins que realment es necessita. Els arxius en format qcow poden contenir una varietat d'imatges de disc que generalment estan associades amb sistemes operatius convidats específics.

Una de les característiques principals de les imatges de disc 'qcow' és que els arxius amb aquest format poden créixer a mesura que s'agreguen dades. Això permet grandàries d'arxiu més petits que les imatges de disc sense processar, ja que aquestes assignen tot l'espai d'imatge a un arxiu, fins i tot si algunes parts estan buides, sent particularment útil per als sistemes d'arxius que no admeten arxius dispersos, com FAT32.

El format 'qcow' també permet emmagatzemar els canvis realitzats en una imatge base de només lectura en un arxiu independent mitjançant l'ús de còpia en escriptura. Aquest arxiu conté la ruta a la imatge base per a poder consultar-la quan sigui necessari. Quan s'ha de llegir una dada particular d'aquesta nova imatge, el contingut es recupera si és nou i es va emmagatzemar allí; si no ho està, les dades es recuperen de la imatge base. Es requereix una utilitat que sigui capaç de llegir arxius qcow abans de poder muntar un. La diferència amb la versió original és que qcow2 admet diverses instantànies utilitzant un model més nou i flexible per a emmagatzemar-les.

Instal·lació de la Màquina Virtual, es pot indicar la capacitat de la imatge i el controlador de la targeta de xarxa que utilitzarà.

```
virt-install \  
--virt-type=kvm \  
--name Firewall \  
--os-type=freebsd \  
--os-variant=freebsd11.2 \  
--ram 1024 \  
--vcpus=1 \  
--cdrom=/var/lib/libvirt/isos/pfSense-CE-2.4.4-RELEASE-p1-amd64.iso \  
--network network=ovs-network-wan,model=rtl8139 \  
--disk path=/var/lib/libvirt/images/Firewall.qcow2,size=4,bus=virtio,format=qcow2
```

Mentre s'inicia el procés d'instal·lació, es poden afegir les interfícies necessàries per a realitzar l'escenari proposat. En primer lloc, cal afegir una nova interfície i assignar-la dins la xarxa LAN.

```
virsh attach-interface --domain Firewall --type network \  
--source ovs-network-lan --model rtl8139 \  
--mac 52:54:00:11:11:11 --config --live
```

En segon lloc, afegir una nova interfície i assignar-la dins la xarxa DMZ.

```
virsh attach-interface --domain Firewall --type network \  
--source ovs-network-dmz --model rtl8139 \  
--mac 52:54:00:33:33:33 --config --live
```

Es pot esborrar una interfície prèviament instal·lada.

```
virsh detach-interface \  
--domain FW --type network \  
--mac 52:54:00:4b:73:5f --config
```

Amb la següent comanda, es mostra la configuració de les interfícies per a cada connexió a les diferents xarxes virtuals del Tallafocs.

```
virsh domiflist FW  
  
Interfaz Tipo Fuente Modelo MAC  
-----  
vnet1 bridge ovs-network-wan rtl8139 52:54:00:75:28:13
```

vnet0 i vnet1 son les interfícies de tap de VM. Quan tanquem aquestes aquestes màquines virtuals, els ports s'eliminaran dels bridges ovs automàticament. Els arxius de registre per a Open vSwitch es guarden en la carpeta '/var/log/openvswitch'.

activar d'inici les VM.

```
systemctl status libvirtd  
  
su  
  
virsh list --all  
  
Id Nombre Estado  
-----  
- FW apagado  
  
virsh autostart FW
```

Una vegada copiats els arxius del sistema al disc dur, es procedeix a configurar les adreces IP de les targetes de xarxa, i es pot accedir al sistema des d'un explorador web. El portal d'administració està basat en PHP i teòricament totes les configuracions i administració es poden realitzar des de l'explorador Web, per tant no és indispensable comptar amb coneixements avançats sobre la línia de comandos UNIX per al seu maneig.

9 Valoració Econòmica

Finalment es dona la valoració econòmica per comprovar si el cost de la solució s'ajusta al pressupost.

Materials per a realitzar el condicionament de la infraestructura de xarxa física:

Elements	Marca i Model	Preu Unitari	unitats	PVP
Rack de comunicacions	Armari rack mural 19" 15U 570x450x790mm	151,99 €	1	151,99 €
Bobina de Cable Cat6	Mr. Tronic Cable de Instal·lació Xarxa Ethernet Bobina 305m CAT6, AWG24, CCA, UTP	75,00 €	1	75,00 €
Connectors RJ45	CableCreation 5-PACK Cat6 / RJ45 Keystone mòdul Connector, Blanc	7,55 €	5	37,75 €
Fuetons	Schneider Electric DC6PCURJ02GYM Fuetó Cat6 UTP 2 m, Gris	6,12 €	32	195,84 €
PatchPannel	RackMatic - Patch panel 24 x RJ45 UTP cat.6 1Gb Ethernet	50,99 €	1	50,99 €
Passafils	Cablematic - Panell guiacables per armari rack 19" de 1U	12,74 €	1	12,74 €
Base d'Endoll per a Rack	RackMatic - Regleta d'endolls per a armari rack 19" 1U amb 8 schuko	25,99 €	1	25,99 €
Total				550,30 €

Taula 2. Desglossament i cost de material, Infraestructura física de Xarxa

Materials per la instal·lació del nous sistemes informàtics mitjançant la virtualització:

Dispositius	Marca i Model	Preu Unitari	unitats	PVP
Servidor per Virtualitzar	DELL PowerEdge R340 Rack Server. Intel® Xeon® E-2176G, Optional Operating System, 16GB Memory, 2TB Hard Drive and a 1 Year Warranty	1.729,00 €	1	1.729,00 €
NAS enrackable	Synology RackStation RS818+, 4 bay	807,30 €	1	807,30 €
HDD NAS	Seagate BarraCuda - Disc dur intern de 5 TB, SATA, 2,5'	181,47 €	2	362,94 €
Acces Point	Ubiquiti Networks Indoor UAP-AC-LR	94,90 €	2	189,80 €
Switch PoE	Netgear GS724TP-200EUS	286,99 €	1	286,99 €
Total				3.376,03 €

Taula 3. Desglossament i cost del Material, Sistemes

Cost total per la adquisició dels materials:

Total, Cost del Materials	
Materials per al condicionament de la infraestructura de xarxa física	550,30 €
Materials per la implantació del Sistemes Informàtics	3.376,03 €
Total	3.926,33 €

Taula 4. Cost total del Material

Per a condicionament de la infraestructura de Xarxa física utilitzarem la figura de Tècnic Especialitzat en cablejat estructurat. Seran els encarregats de la Instal·lació del nou armari, dels punts d'accés a la xarxa sense fils i realitzaran els accions pertinents per a optimitzar el cablejat de la xarxa.

Tècnic especialista en estructura física de Xarxes			
Preu Hora	30		
Tasques	nº hores	PVP	
Instal·lació del Rack de Comunicacions	6	180,00 €	
Condicionament del Cablejat Estructurat	12	360,00 €	
Instal·lació dels Accés Points	4	120,00 €	
Total	20	660,00 €	

Taula 5. Desglossament i cost de tasques, Tècnic especialista

Per a la Instal·lació i Configuració del nou Sistema Informàtic utilitzarem les figures d'Administrador de Sistemes i Tècnic de Sistemes. L'Administrador de Sistemes presentarà el plantejament de tot el sistema, detallarà quins son els elements necessaris per construir la nova estructura i posarà en marxa a els procediments per que siguin implementats pels diferents departaments Tècnics.

Administrador de Sistemes			
Preu Hora	80		
Tasques	nº hores	PVP	
Estudi i realització del informe	8	640,00 €	
Total	8	640,00 €	

Taula 6. Desglossament i cost de tasques, Administrador de Sistemes

D'altra banda, la figura de Tècnic de Sistemes serà l'encarregada de modelar tot l'equipament informàtic, realitzar en el NAS i al servidor de virtualització tota la configuració, i instal·lar i configurar les màquines virtuals. Finalment, configurarà les xarxes del Hipervisor, del Tallafocs i del commutador físic.

Tècnic de Sistemes		
Preu Hora	60	
Tasques	nº hores	PVP
Preparació del Servidor	2	120,00 €
Instal·lació del Sistema Operatiu	1	60,00 €
Configuració de la Xarxa a l'Hipervisor	4	240,00 €
Instal·lació de les màquines Virtuals	2	120,00 €
Configuració del Tallafocs	9	540,00 €
Configuració del Servidor FTP	2	120,00 €
Configuració del Servidor Web	2	120,00 €
Configuració del Servidor de Domini	7	420,00 €
Preparació i configuració del Switch	2	120,00 €
Configuració dels Acces Points	2	120,00 €
Preparació del NAS	2	120,00 €
Configuració de las funcionalitats del NAS	5	300,00 €
	Total	40
		2.400,00 €

Taula 7. Desglossament i cost de tasques, Tècnic de Sistemes

Cost total per la contractació del personal, sumatori de les tres figures necessàries:

Total, Cost del Personal	
Cost del Personal Tècnic especialitzat	660,00 €
Cost del Personal Administració de Sistemes	640,00 €
Cost del Personal Tècnic de Sistemes	2.400,00 €
Total	3.700,00 €

Taula 8. Cost total del Personal

Per definir el cost total de tot el projecte sumarem cadascú dels costos del Material y del Personal:

Cost Total del Projecte	
Total, Materials	3.926,33 €
Total, Cost del Personal	3.700,00 €
Total	7.626,33 €

Taula 9. Cost total del projecte

El projecte per BAIXLIGHTS té un pressupost de 10.000 €, la solució encaixa, encara quedaria un romanent de 2373,67 €.

10 Conclusions

En aquest apartat es descriuen la conclusions d'aquest treball:

- He pogut comprovar quins són els processos que porten a definir un projecte a partir d'una idea. He conegut la manera de identificar una situació a la qual se li ha de proposar una solució.
- He après que no totes les solucions poden resoldre els mateixos problemes. Cal trobar quina és la solució més propícia per a resoldre determinat problema i plantejar el anàlisis de manera que pugui visualitzar les diferents opcions disponibles.

S'ha pogut aconseguir els objectius plantejats en un inici, encara que en un moment determinat de l'elaboració del projecte ha estat necessari reorientar-los, en un principi estaven més encaminats a la solució enlloc del plantejament.

- S'ha trobat una solució de confiança per a contrarestar l'obsolescència del maquinari mitjançant la virtualització i el programari no propietari.
- El cost de la solució no ha suposat més de 10.000€. Finalment hem assolit l'objectiu amb uns costos de 7.626,33 €

Es poden afegir altres consideracions de objectius amb menys rellevància:

- S'han estudiat diferents mètodes per a crear escenaris propis virtualitzats. Es un dels objectius que han portat a seleccionar la temàtica d'aquest TFG.
- S'han identificar els diferents mecanismes que possibiliten que els convidats virtualitzats es comuniquin amb les interfícies de xarxa. He pogut comprovar que la integració de KVM amb Open vSwitch ofereix millor rendiment que les eines que disposa KVM. En el moment de connectar les màquines virtuals a diferents xarxes l'Hipervisor sofreix alteracions en el seu funcionament.

La planificació no ha estat tot l'òptima que hauria d'haver estat, Es va planificar massa temps en l'estudi de la solució, i no es va tenir en compte alguns dels passos necessaris per a consolidar el projecte. Em refereixo al fet que no es van poder definir alguns punts dels plantejaments, justificacions i

l'anàlisi de la situació, encara que no hi ha hagut desviaments significatius que hagin provocat canvis en la solució proposada.

Al realitzar una solució per a oferir els serveis mitjançant un cost assequible, les línies de futur que no s'han pogut abordar i que penso que són necessàries, estan enfocades a oferir més característiques a la infraestructura de la empresa. Es poden afegir nous serveis que aportin a la infraestructura característiques que en aquest moment no es donen. El projecte es limita a mantenir els serveis, millorant la infraestructura física de xarxa i afegint un element que proporciona seguretat a un nivell general.

11 Glossari

Bridge.- És un dispositiu d'interconnexió de xarxes d'ordinadors que opera a nivell d'enllaç de dades del model OSI. Aquest interconnecta dos segments de xarxa fent el passatge de dades d'una xarxa a l'altre, amb base de la direcció física de destí de cada paquet.

Cloud computing.- És una forma de computació que té els seus fonaments a Internet i que mitjançant la qual, els recursos compartits, programari i informació, es proporcionen a ordinadors i d'altres dispositius a la carta com a serveis.

Commutador en xarxa.- (en anglès **network switch**) és un aparell de xarxes que permet agrupar un conjunt d'ordinadors i fer que passin pel mateix cable. A diferència dels concentradors, per cada paquet que hi arriba, el commutador l'envia només al seu destí.

DMZ.- En termes de seguretat informàtica, una **DMZ** o **zona desmilitaritzada** és una subxarxa d'àrea local, LAN, situada entre la xarxa privada d'una organització i la xarxa externa, normalment Internet.

Ethernet.- és una tecnologia de xarxa de computadors d'àrea local desenvolupada als anys 70 al Xerox PARC, per Robert Metcalfe. Aquest té accés al medi per contingut CSMA/CD.

Gateway.- És un dispositiu que permet interconnectar xarxes que utilitzen arquitectures o protocols diferents, és una porta d'enllaç en una xarxa.

Guest.- o **convidat**, en l'àmbit de la virtualització, un convidat s'executa en el host utilitzant recursos compartits donats pel host.

Hipervisor.- (en anglès *hypervisor*) o monitor de màquina virtual és una plataforma que permet aplicar diverses tècniques de control de virtualització per a la seva utilització, diferents sistemes operatius en una mateix maquinari.

Host.- o **amfitrió**, en l'àmbit de la virtualització, és el maquinari subjacent que proporciona recursos informàtics a les màquines virtuals, com la potència de processament, la memòria i el disc.

Kernel.- El nucli del sistema operatiu és la part fonamental d'un sistema operatiu. És el programari responsable de facilitar als diversos programes accés segur al maquinari de l'ordinador.

Màquina virtual.- és un programari que emula un ordinador i pot executar programes com si fos un ordinador real tot i que està virtualitzat. Aquest programari en un principi va ser definit com 'un duplicat eficient i aïllat d'una màquina física'.

NAS.- (en anglès Network Attached Storage) és el nom donat a una tecnologia d'emmagatzematge dedicada a compartir la capacitat d'emmagatzematge d'un Servidor i ordinadors personals a través d'una xarxa, fent ús d'un sistema operatiu

Obsolescència.- És la condició o estat en què es troba un producte que ja ha complert amb una vigència o temps programat perquè continuï funcionant.

Shell.- és una peça de programari que proporciona una interfície als usuaris. Típicament, el terme es refereix a una shell d'un sistema operatiu que proporciona accés als serveis del kernel.

Tallafocs.- (en anglès **Firewall**) és un element de maquinari o programari utilitzat en una xarxa d'equips informàtics per controlar les comunicacions, permetent-les o prohibint-les segons les polítiques de xarxa que hagi definit l'organització responsable de la xarxa.

Virtualització.- és un mecanisme que permet compartir una màquina física per executar diverses màquines virtuals que consisteixen en sistemes operatius. Aquestes màquines virtuals comparteixen els recursos lliures de CPU, memòria, disc i connexió de xarxa.

Vlan.- (acrònim de virtual LAN, xarxa d'àrea local virtual) és un mètode de crear xarxes lògicament independents dins d'una mateixa xarxa física.

12 Bibliografia

1. KUMAR, P. "How to Install and use open vSwitch 2.9 with KVM on CentOS7 / RHEL 7 Server". [en línia] A: **LinuxTechi: Linux tutorials & guide**, 2018. <<https://www.linuxtechi.com/install-use-openswitch-kvm-centos-7-rhel-7/>> [Consulta: 10 maig 2019]
2. LIU, Hangbin. "Introduction to Linux interfaces for virtual networking". [en línia] A: **Red Hat Developer, Blog Articles** 2018. <<https://developers.redhat.com/blog/2018/10/22/introduction-to-linux-interfaces-for-virtual-networking/>> [Consulta: 3 maig 2019]
3. "The CentOS Project". [en línia] A: **The CentOS Project** 2019. <<https://www.centos.org/>> [Consulta: 10 abril 2019]
4. M. Tim Jones. "La anatomía de un hipervisor Linux". [en línia] A: **IBM** 2009. <<https://www.ibm.com/developerworks/ssa/library/l-hypervisor/index.html#artrelatedtopics>> [Consulta: 15 abril 2019]
5. FERNÁNDEZ DUQUE, Víctor. "Desarrollo de un entorno de vitalització de redes con fines docentes". [en línia]. A: **E-Prints Complutense**. Madrid: Universidad Complutense, 2018. 61 p. [Trabajo fin de Grado] <<https://eprints.ucm.es/48848/1/037.pdf>> [Consulta: 14 maig 2019]
6. PHILLED (Pseudònim). "How to activate multiple NICs (KVM)?" [en línia] A: **Ubuntu forums**, 2016. <<https://ubuntuforums.org/showthread.php?t=2309132>> [Consulta: 30 maig 2019]
7. "KVM and Oracle VM VirtualBOX". [en línia]. Nova York: IT Central Station, 2019. (Buyer's Guide and Reviews) <<https://bit.ly/2MBoBNa>> [Consulta: 30 maig 2019]
8. PELÚS, Bernabé. "Configurar las interfases de Red en Centos 7" [en línia] A: **Grupotelfor: cloud hosting Technology**. Alicante: Grupotelfor. (Post del dia 20/04/2017) <<http://www.grupotelfor.com/blog/7-centos-7/8-configurar-las-interfases-de-red-en-centos-7>> [Consulta: 12 maig 2019]

13 Annexos

13.1 Arxius de configuració de les interfícies virtuals

ovs-br-wan

```
nano /etc/sysconfig/network-scripts/ifcfg-ovs-br-wan

TYPE=OVSBridge
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
DEFROUTE="no"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="no"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
IPV6_PRIVACY="no"
NAME=ovs-br-wan
DEVICE=ovs-br-wan
DEVICETYPE="ovs"
ONBOOT="yes"
IPADDR="192.168.1.254"
PREFIX="24"
GATEWAY="192.168.1.1"
```

ovs-br-lan

```
nano /etc/sysconfig/network-scripts/ifcfg-ovs-br-lan

TYPE=OVSBridge
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
DEFROUTE="no"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="no"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
IPV6_PRIVACY="no"
NAME=ovs-br-lan
DEVICE=ovs-br-lan
DEVICETYPE="ovs"
ONBOOT="yes"
IPADDR="172.16.0.254"
PREFIX="24"
GATEWAY="172.16.0.1"
```

ovs-br-dmz

```
nano /etc/sysconfig/network-scripts/ifcfg-ovs-br-dmz

TYPE=OVSBridge
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
DEFROUTE="no"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="no"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
IPV6_PRIVACY="no"
NAME=ovs-br-dmz
DEVICE=ovs-br-dmz
DEVICETYPE="ovs"
ONBOOT="yes"
IPADDR="10.0.0.254"
PREFIX="24"
GATEWAY="10.0.0.1"
```

13.2 Arxius de configuració de les interfícies físiques

eno1

```
nano /etc/sysconfig/network-scripts/ifcfg-eno1

TYPE=OVSPort
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="eno1"
DEVICETYPE="ovs"
OVS_BRIDGE="ovs-br-wan"
DEVICE="eno1"
ONBOOT="yes"
HWADDR=f0:92:1c:e3:4c:54
IPADDR="192.168.1.253"
PREFIX="24"
GATEWAY="192.168.1.1"
DNS1="8.8.8.8"
```

enp2s0

```
nano /etc/sysconfig/network-scripts/ifcfg-enp2s0

TYPE="OVSPort"
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE="no"
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=no
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp2s0
DEVICETYPE="ovs"
OVS_BRIDGE="ovs-br-lan"
DEVICE=enp2s0
ONBOOT="yes"
HWADDR="68:05:ca:93:aa:72"
IPADDR="172.16.0.253"
PREFIX="24"
GATEWAY="172.16.0.1"
```

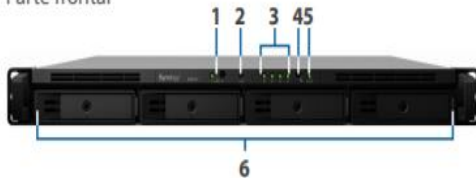
13.3 Especificacions, DELL Power Edge R340 enrackable

PowerEdge R340		
Features	Technical Specification	
Processor	1 processor from the following: Intel® Xeon® E-2100 product family, Intel Pentium®, Intel Core i3®, Intel Celeron®	
Memory	4 x DDR4 DIMM slots, Supports UDIMM, up to 2666MT/s, 64GB Max. Supports registered ECC	
Storage controllers	Internal controllers: PERC H730P, H330, HBA330 (non-RAID) Software RAID: PERC S140 External HBAs: 12Gbps SAS HBA (non-RAID) Boot Optimized Storage Subsystem: 2x M.2 240GB (RAID 1 or No RAID), 1x M.2 240GB (No RAID only)	
Drive bays	Up to 8 x 2.5 hot-plug SATA, SAS (optional) or SSD Up to 4 x 3.5 hot-plug SATA, SAS (optional) or SSD	
Power supplies	Single or dual 350W (Platinum) or 550W (Platinum) hot-plug redundant power supplies	
Dimensions	Form factor: Rack (1U)	Chassis width: 434.00mm (17.08 in) Chassis depth: 595.63mm (23.45 in) (3.5" HHD config) Chassis depth: 544.836mm (21.45 in) (2.5" HHD config) Note: These dimensions do not include: bezel, redundant PSU Chassis weight: 13.6 kg (29.98 lb.)
Embedded management	iDRAC9 with Lifecycle Controller iDRAC Direct iDRAC RESTful API with Redfish	
Bezel	Optional security bezel	
OpenManage™ Software	OpenManage Enterprise OpenManage Essentials	OpenManage Power Center OpenManage Mobile (requires OpenManage Enterprise)
Integrations and connections	Integrations: Microsoft® System Center VMware® vCenter™ BMC Truesight (available from BMC) Red Hat Ansible	Connections: Nagios Core & Nagios XI Micro Focus Operations Manager i (OMI) IBM Tivoli Netcool/OMNIBus
Tools	iDRAC Service Module OpenManage Server Administrator Dell EMC Repository Manager Dell EMC System Update	Dell EMC Server Update Utility Dell EMC Update Catalogs Dell EMC RACADM CLI IPMI Tool
Security	TPM 1.2/2.0 optional Cryptographically signed firmware Silicon Root of Trust	Secure Boot System Lockdown (requires OpenManage Enterprise) System Erase
I/O & Ports	Networking Options: 2 x 1GbE LOM Network Interface Controller (NIC) ports Front ports: 1x USB 2.0, 1 x iDRAC micro USB 2.0 management port Rear ports: 2 x USB 3.0, VGA, serial connector	2 x PCIe Gen 3.0 slots: • One x8 slot low-profile, half-length with x4 slot width • One x16 slot low-profile/full-height, half-length with x8 bandwidth
Supported operating systems	Certify XenServer Citrix® XenServer® Microsoft Windows Server® with Hyper-V Red Hat® Enterprise Linux Ubuntu Server	SUSE® Linux Enterprise Server VMware® ESXi For specifications and interoperability details, see Dell.com/OSsupport .
OEM-ready version available	From bezel to BIOS to packaging, your servers can look and feel as if they were designed and built by you. For more information, visit Dell.com/OEM .	
Recommended support	ProSupport Plus for critical systems or ProSupport for comprehensive hardware and software support for your PowerEdge solution. Consulting and deployment offerings are also available. Contact your Dell EMC representative today for more information. Availability and terms of Dell EMC Services vary by region. For more information, visit Dell.com/ServiceDescriptions .	
Dell Financial Services	Deliver results with easy financing. Explore financial options that move at the speed of business. For more information, visit https://www.emc.com/products/how-to-buy/global-financial-services/index.htm .	

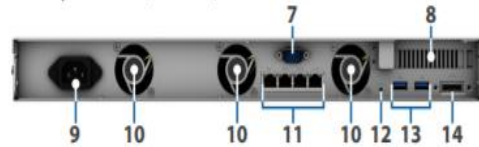
13.4 Especificaciones, Synology NAS

Descripción del hardware

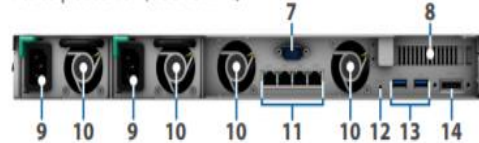
Parte frontal



Parte posterior (RS818+)



Parte posterior (RS818RP+)



1	Botón e indicador de alimentación	2	Indicador de alerta	3	Indicador de estado del disco	4	Botón de pitido desactivado
5	Indicador de estado	6	Bandeja de discos	7	Puerto de consola	8	Ranura de expansión PCIe
9	Puerto de alimentación	10	Ventilador	11	Puerto RJ-45 1GbE	12	Botón RESET
13	Puerto USB 3.0	14	Puerto de expansión				

Especificaciones técnicas

Hardware

CPU	Intel Atom C2538 de cuatro núcleos 2,4 GHz
Motor de cifrado de hardware	SI (AES-NI)
Memoria	2 GB de DDR3L no ECC SO-DIMM (ampliable a 16 GB con 2 x 8 GB SO-DIMM)
Tipo de disco compatible	4 x SSD/HDD SATA de 3,5" o 2,5" (no se incluyen los discos)
Disco intercambiable en caliente	Sí
Puerto externo	<ul style="list-style-type: none"> • 2 x puerto USB 3.0 • 1 x puerto de expansión
Tamaño (Al. x An. x Pr.)	<ul style="list-style-type: none"> • RS818+: 44 x 430,5 x 457,6 mm/44 x 480 x 492,6 mm (con las aletas del servidor) • RS818RP+: 44 x 430,5 x 483,6 mm/44 x 480 x 518,6 mm (con las aletas del servidor)
Peso	<ul style="list-style-type: none"> • RS818+: 6,21 kg • RS818RP+: 7,63 kg
LAN	4 x 1 GbE (RJ-45)
Wake on LAN/WAN	Sí
Ranura PCIe 2.0	<ul style="list-style-type: none"> • 1 ranuras de 4 carriles x8 • Compatibilidad con tarjeta de interfaz de red de alto rendimiento
Encendido/apagado programado	Sí
Ventilador del sistema	<ul style="list-style-type: none"> • RS818+: 3 (40 x 40 x 20 mm) • RS818RP+: 2 (40 x 40 x 20 mm)
Tensión de alimentación de entrada CA	de 100 a 240 V CA
Frecuencia de alimentación	50/60 Hz, monofásica
Temperatura de funcionamiento	De 5 °C a 35 °C (de 40 °F a 95 °F)
Temperatura de almacenamiento	de -20 °C a 60 °C (de -5 °F a 140 °F)
Humedad relativa	Del 5 al 95 % de HR
Altitud operativa máxima	5000 m (16 400 pies)