



## **PROYECTO FINAL DE CARRERA**

**TÍTULO:** Análisis, diseño e implementación de infraestructura de red y de procesamiento centralizado de aplicaciones de laboratorio.

**UNIVERSIDAD:** Universidad Tecnológica Nacional, Facultad Regional Santa Fe.

**ALUMNO:** Matías Santiago López.

**DIRECTORA:** Ing. María Celeste Weidmann.

**AÑO:** 2018.

## Indice

<b>Introducción</b>	<b>6</b>
Temática del proyecto	6
Contexto/Problema	7
Objetivos y Alcance	7
Objetivos Generales	8
Objetivos Específicos	8
Organización del informe	8
Marco teórico introductorio	<b>9</b>
Posibilidades que nos provee la virtualización	9
Virtualización de servidores	9
Virtualización de la red	10
Almacenamiento definido por el software	10
Virtualización de escritorios y aplicaciones	10
Infraestructura	11
Infraestructura Física	11
Infraestructura Virtual	11
Comparación Infraestructura virtual y fisica	12
Compartición de recursos	13
Virtualización de CPU	14
Uso de memoria en host físicos y virtualizados	15
Networking en host físicos y virtuales	15
Etapa 1: Infraestructura de virtualización	<b>16</b>
Análisis de requerimientos de hardware de las aplicaciones	16
Estudio y elección de plataforma de procesamiento virtualizado	18
Citrix Xenserver	18
Microsoft Hyper-V	20
PROXMOX VE	23
Comparación de las diversas herramientas	25
Análisis de requerimientos de hardware para clúster	32
Definición y estructura de un clúster	32
Diseño del clúster	32

Diseño de clúster de procesamiento en alta disponibilidad	34
Arquitectura del Clúster	34
Hardware empleado	36
Implementación de infraestructura de cluster de servidores	37
<b>Etapa 2: Sistemas Operativos y colecciones de software</b>	<b>38</b>
Análisis, diseño e implementación de arquitectura de procesamiento remoto	38
Arquitectura de Virtualización de Aplicaciones	39
Diseño e implementación de RDS	42
Creación de máquinas virtuales y colecciones de software	43
Los RDSHs	43
Las colecciones de software	44
Estudio e implementación de servidor de licencias flotantes	44
Servidor de licencias de escritorio remoto (RDL)	44
Servidor de licencias para aplicaciones (ALS)	45
NLM Flexera	46
Diseño y creación de perfiles de acceso a los software (Active Directory)	48
Active Directory	49
Funcionamiento	50
Diseño e implementación de seguridad en sistemas operativos (Firewall, Backups)	50
Firewall	50
Backups	51
Primer etapa de pruebas de rendimiento	52
Pruebas con aplicación Simio 6	52
Pruebas con aplicación Autocad 2018	53
Conclusiones de las pruebas	53
<b>Etapa 3: Infraestructura de red</b>	<b>54</b>
Diseño e implementación de topología de red de servidores de procesamiento remoto	54
Diseño e implementación de topología de red de clientes (servidor DHCP)	55
Diseño lógico de la red de clientes	55
Diseño físico de la red clientes	55
Diseño y configuración de puntos de acceso inalámbrico a la red de clientes	57
Análisis, diseño e implementación de seguridad en las redes (Access Control List)	59

Segunda etapa de pruebas de rendimiento	62
Pruebas con aplicación Simio 6	62
Pruebas con aplicación Autocad 2018	63
Conclusiones de las pruebas	63
Extensibilidad	<b>64</b>
Conclusiones	<b>64</b>
Referencias bibliográficas	<b>65</b>
Anexos	<b>67</b>
Instalación de PROXMOX VE	68
Creación del Cluster	73
Creación del Bond	74
Creación de VLAN Bridge	76
Activación de forwarding	77
Configuración de MTU en interfaces	77
Conexión de Storage	78
Montar directorio compartido	80
Backups y reducción de velocidad	82
HA - comandos e inicio del servicio	83
Configuración de Switch de arquitectura de virtualización	84
Configuración de Switch de Intranet	84
Configuración de Switches de iSCSI	85
Configuración de Switch de Núcleo	86
Configuración de Storage	88
Implementación de roles de RDS en Windows Server	90
Instalación y configuración de RDL	97
Activación de RDL	100
Instalación de Licencias	105
Agregar el servidor de licencias a Active Directory	109
Agregar el servidor de licencias al entorno RDS	112
Publicación de aplicaciones	115
Configuración de NLM Flexera	122
Implementación de Rol de AD en Windows Server	125

Creación de contenedores, usuarios y grupos.	126
Configuración de Firewall de Windows	127
Configuración de backups en Proxmox	128
Implementación de Rol de NFS en Windows Server	129
Configurar un recurso compartido NFS	131
Gráficas de la primer etapa de pruebas	133
Pruebas sobre el software Simio 6	133
Uso de procesador en servidores RDSH1 y RDSH2	134
Uso de memoria en servidores RDSH1 y RDSH2	135
Uso de red en RDSH1 y RDSH2	136
Uso de red en switch de acceso	137
Pruebas sobre el software Autocad 2018	138
Uso de procesador en servidores RDSH1 y RDSH2	139
Uso de memoria en servidores RDSH1 y RDSH2	140
Uso de red en servidores RDSH1 y RDSH2	141
Uso de red en switch de acceso	142
Configuraciones de red Wifi	143
Listas de Control de Acceso	144
Pautas generales para la creación de una ACL	144
Dónde ubicar las ACL	145
Gráficas de la segunda etapa de pruebas	146
Pruebas sobre el software Simio 6	146
Uso de procesador en servidores RDSH1 y RDSH2	147
Uso de procesador en Access Point	148
Uso de memoria en servidores RDSH1 y RDSH2	149
Uso de memoria en Access Point	150
Uso de red en servidores RDSH1 y RDSH2	151
Uso de red en Access Point	152
Pruebas sobre el software Autocad 2018	153
Uso de procesador en servidores RDSH1 y RDSH2	154
Uso de procesador en Access Point	155
Uso de memoria en servidores RDSH1 y RDSH2	156
Uso de memoria en Access Point	157

Uso de red en servidores RDSH1 y RDSH2	158
Uso de red en Access Point	159

# 1. Introducción

## 1.1. Temática del proyecto

“La virtualización es una tecnología probada de software que permite ejecutar múltiples sistemas operativos y aplicaciones simultáneamente en un mismo servidor. Está transformando el panorama de TI<sup>1</sup> y modificando totalmente la manera en que las personas utilizan la tecnología”.[1]

“Podemos definir a la virtualización como la creación (a través de software) de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red”.[2]

Dicho de otra manera, se refiere a la abstracción de los recursos de una computadora, llamada Hipervisor o VMM<sup>2</sup> que crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest), dividiéndose el recurso en uno o más entornos de ejecución.

Esta capa de software VMM maneja, gestiona y arbitra los cuatro recursos principales de una computadora (CPU<sup>3</sup>, Memoria, Dispositivos Periféricos y Conexiones de Red) y así puede repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. Esto hace que se puedan tener varios ordenadores virtuales ejecutándose en el mismo ordenador físico.

Existen diferentes formas de virtualización: es posible virtualizar el hardware de servidor, el software de servidor, virtualizar sesiones de usuario, virtualizar aplicaciones y también se pueden crear máquinas virtuales en una computadora de escritorio.[4]

La virtualización de aplicaciones permite la ejecución remota de una aplicación por medio de una pc cliente en una arquitectura que se define Cliente-Servidor. Esta arquitectura nos permite centralizar la ejecución de las aplicaciones en clusters de servidores diseñados específicamente para soportar la ejecución de múltiples instancias simultáneamente. El

---

<sup>1</sup> TI: Tecnología de la Información.

<sup>2</sup> VMM, por sus siglas en inglés: Virtual Machine Manager.

<sup>3</sup> CPU, por sus siglas en inglés: Central Process Unit.

Ciente, llamado terminal “boba” en ocasiones, es una pc que sólo se encarga de presentar en su pantalla los resultados de el procesamiento de la aplicación realizado por el Servidor.

## **1.2. Contexto/Problema**

Con frecuencia las cátedras de las diversas carreras de la facultad hacen uso de software licenciado como apoyo al dictado de las asignaturas. Tanto desde Rectorado de la Universidad Tecnológica Nacional, como desde las mismas cátedras se gestiona la obtención de las distintas licencias para su uso en las computadoras de los laboratorios informáticos, siendo la adquisición de licencias personales para uso de los alumnos responsabilidad de los mismos. La facultad sólo ofrece la posibilidad de acceder a la utilización de los software en los laboratorios y en los horarios reservados para tal fin.

Debido a que los requerimientos de hardware de muchos software se incrementa rápidamente, el ciclo de vida útil de los equipos informáticos cada vez es menor y surge la necesidad de actualizarlos con mayor frecuencia.

## **1.3 Objetivos y Alcance**

El presente proyecto tiene como objetivo eliminar la limitación de la disponibilidad física de los laboratorios informáticos para el desarrollo de las actividades de las cátedras, como así también otorgar la posibilidad de la utilización de los software por parte de estudiantes y docentes con equipos personales dentro de las instalaciones de la facultad.

Desde el punto de vista de los recursos tecnológicos, creemos que la centralización del procesamiento de las aplicaciones puede hacer un uso más eficiente de los recursos humanos y tecnológicos involucrados, facilitando tareas de mantenimiento y gestión sobre el hardware, como así también postergando el umbral de obsolescencia de los equipos informáticos de laboratorio.



El Alcance de este proyecto abarca el diseño e implementación de un Clúster de Servidores, una arquitectura de procesamiento centralizado de aplicaciones y una topología de red de base para la comunicación de clientes y servidores en el entorno de la UTN FRSF<sup>4</sup>.

### **1.3.1 Objetivos Generales**

Diseñar e implementar una infraestructura de servidores y redes que posibilite el acceso a docentes y alumnos de la UTN FRSF a los diversos software utilizados en el dictado de las cátedras, en las instalaciones de la facultad y con cualquier computadora.

### **1.3.2 Objetivos Específicos**

- Permitir el acceso a alumnos y docentes de la comunidad académica a distintas colecciones de software desde sus computadoras personales.
- Permitir el desarrollo de actividades académicas de laboratorio en aulas de la facultad inicialmente no destinadas a tal fin.
- Centralizar el procesamiento de aplicaciones de modo de independizar las mismas de los equipos utilizados por los usuarios.
- Centralizar la gestión de los recursos tecnológicos de la facultad.
- Disminuir las limitaciones asociadas a la disponibilidad de recursos tecnológicos.
- Explotar el uso de la infraestructura de redes existente en la facultad.
- Implementar una infraestructura de procesamiento escalable.

## **1.4 Organización del informe**

La estructura del presente informe se centra en tres capítulos en los cuales se desarrollan todos los aspectos técnicos del proyecto. Al comienzo de cada capítulo se hará una breve introducción a la temática que se trata en el mismo, de modo de tener una base de conocimiento que ayude al entendimiento de los temas desarrollados.

En el primer capítulo se desarrolla todo lo relacionado al diseño e implementación de una infraestructura de virtualización de servidores. El resultado de este capítulo debería servir de

---

<sup>4</sup> UTN FRSF: Universidad Tecnológica Nacional, Facultad Regional Santa Fe.

guía para diseñar una Infraestructura de Virtualización en función de los requerimientos de las aplicaciones que se quieran procesar.

En el segundo capítulo se lleva a cabo el diseño e implementación de una arquitectura de procesamiento remoto. Abarca aspectos que van desde la topología de procesamiento, licencia, servidor de licencias de aplicaciones, hasta seguridad de sistemas operativos. El resultado de este capítulo es presentar una arquitectura de procesamiento centralizado de aplicaciones de escritorio.

En el tercer capítulo se desarrolla el estudio, diseño e implementación de la topología de red lógica para servidores y usuarios. En esta sección se abarcan todos los aspectos relacionados a la seguridad de las redes LAN<sup>5</sup> y WLAN<sup>6</sup> involucradas. Este capítulo tiene por objetivo presentar el diseño de red necesario para dar soporte a toda la infraestructura desarrollada en los capítulos anteriores.

Finalmente, el cuarto capítulo está dedicado a las conclusiones sobre el trabajo realizado basándonos en las experiencias recabadas tanto durante el desarrollo de proyecto como en su puesta en producción.

## **2. Marco teórico introductorio**

### **2.1. Posibilidades que nos provee la virtualización**

#### **2.1.1. Virtualización de servidores**

“La mayoría de los servidores funcionan a menos del 15 % de su capacidad, lo que causa la expansión de servidores y aumenta la complejidad. Gracias a la virtualización de servidor, se abordan estas ineficiencias mediante la ejecución de varios sistemas operativos en un único servidor físico como máquinas virtuales, y cada una de ellas tiene acceso a los recursos de procesamiento del servidor subyacente. Sin embargo, la virtualización de uno o dos servidores es solo el comienzo. El paso siguiente es agregar un clúster de servidores a un recurso único y consolidado, gracias a lo cual se aumenta la eficacia general y se reducen los

---

<sup>5</sup> LAN, por sus siglas en inglés: Local Area Network.

<sup>6</sup> WLAN, por sus siglas en inglés: Wireless Local Area Network.

costos. La virtualización de servidor también permite una implementación de cargas de trabajo más rápida, un aumento del rendimiento de las aplicaciones y una disponibilidad superior. Además, a medida que las operaciones se automatizan, la administración de TI se simplifica y la operación y propiedad se vuelven menos costosas.

### **2.1.2. Virtualización de la red**

La virtualización de redes es la reproducción completa de una red física en software. Las aplicaciones se ejecutan en la red virtual exactamente del mismo modo en que lo hacen en una red física. La virtualización de red presenta dispositivos y servicios de red lógicos, es decir, puertos lógicos, switches, enrutadores, firewalls, equilibradores de carga, redes privadas virtuales (VPN, Virtual Private Network) y mucho más, para cargas de trabajo conectadas. Las redes virtuales ofrecen las mismas funciones y garantías que una red física, junto con las ventajas operacionales y la independencia de hardware propias de la virtualización.

### **2.1.3. Almacenamiento definido por el software**

Los grandes volúmenes de datos y las aplicaciones en tiempo real están llevando las demandas de almacenamiento a nuevos niveles. Mediante la virtualización del almacenamiento, se separan los discos y las unidades flash en los servidores, se los combina en depósitos de almacenamiento de alto rendimiento y se los suministra como software. El almacenamiento definido por el software (SDS, Software Defined Storage) es una nueva estrategia para el almacenamiento que brinda un modelo operacional fundamentalmente más eficaz.

### **2.1.4. Virtualización de escritorios y aplicaciones**

La implementación de escritorios como un servicio administrado permite responder con mayor rapidez a las necesidades y las oportunidades cambiantes. Puede reducir costos y aumentar el servicio mediante el suministro rápido y sencillo de escritorios y aplicaciones virtualizadas a las sucursales, a los empleados en el extranjero y tercerizados.”[5]

## **2.2. Infraestructura**

### **2.2.1. Infraestructura Física**

Tradicionalmente, los sistemas operativos y el software corrían en computadoras físicas. Existen varios desafíos para correr un gran número de servidores físicos en un datacenter. El modelo no es flexible y puede ser ineficiente. La planificación y el costo de infraestructura adecuada son sólo algunos de los problemas que el personal de TI debe abordar.

Generalmente, existe una relación 1:1 entre una computadora física y el software que corre en la misma. Esta relación deja la mayoría de las PC<sup>7</sup> infrutilizadas. El costo de este espacio y la energía requerida para alojarlas, ejecutarlas y mantenerlas refrigeradas puede ser expansivo.

El aprovisionamiento de servidores físicos es un proceso que consume tiempo. En entornos no virtualizados el tiempo que lleva adquirir nuevo hardware, colocarlo en el centro de datos, instalarle un sistema operativo, parchear el sistema operativo e instalar y configurar las aplicaciones requeridas puede tomar semanas. Además de este proceso, se debe considerar la integración del nuevo equipo a la infraestructura existente. Por ejemplo, la configuración de reglas de firewall, habilitación de puertos de switch y el aprovisionamiento de almacenamiento.

### **2.2.2 Infraestructura Virtual**

Una infraestructura virtual consiste en el mapeo dinámico de recursos físicos en función de las necesidades de la empresa. Una máquina virtual representa los recursos físicos de un único ordenador, mientras que una infraestructura virtual representa los recursos físicos de la totalidad del entorno de TI, aglutinando ordenadores x86, así como su red y almacenamiento asociado, en un pool unificado de recursos de TI.

Estructuralmente, una infraestructura virtual consta de los siguientes componentes:

---

<sup>7</sup> PC, por sus siglas en inglés: Personal Computer.

- Hipervisor de un solo nodo para hacer posible la virtualización de todos los ordenadores x86.
- Un conjunto de servicios de infraestructura de sistemas distribuida basada en la virtualización, para optimizar los recursos disponibles entre las máquinas virtuales.
- Soluciones de automatización que proporcionen capacidades especiales para optimizar un proceso de TI concreto, como el aprovisionamiento o recuperación ante desastres.

Mediante la separación de la totalidad del entorno de software de su infraestructura de hardware subyacente, la virtualización hace posible la reunión de varios servidores, estructuras de almacenamiento y redes en pools compartidos de recursos que se pueden asignar de forma dinámica, segura y fiable a las aplicaciones según sea necesario. Este enfoque innovador permite a las organizaciones crear una infraestructura informática con altos niveles de utilización, disponibilidad, automatización y flexibilidad utilizando componentes básicos de servidores económicos y estándar del sector.[3]

### **2.2.3 Comparación Infraestructura virtual y física**

La virtualización proporciona una solución a muchos de los problemas con que se encuentra el personal de TI. La virtualización es una tecnología que desacopla el hardware físico del sistema operativo. Permite consolidar y ejecutar múltiples cargas de trabajo como máquinas virtuales en un solo ordenador. Una máquina virtual es un equipo que está creado por software que, al igual que un equipo físico, ejecuta un sistema operativo y aplicaciones. Cada máquina virtual contiene su propio hardware virtual, incluyendo CPU virtual, memoria, disco duro e interfaces de red, que para el sistema operativo y las aplicaciones se parecen al hardware físico.

Los gráficos que se muestran en la figura 1 ilustran las diferencias entre un host virtualizado y uno no virtualizado. En las arquitecturas tradicionales, el sistema operativo interactúa directamente con el hardware instalado. Éste es el que organiza los procesos en ejecución, asigna memoria a las aplicaciones, envía y recibe datos en las interfaces de red y lee y escribe en los dispositivos de almacenamiento que tiene conectado. En comparación, un host virtualizado interactúa con el hardware instalado a través de una fina capa de software

llamada capa de virtualización o hipervisor. El hipervisor ofrece dinámicamente recursos de hardware físicos a las máquinas virtuales, según lo necesiten. El hipervisor permite a las máquinas virtuales operar con un grado de independencia del hardware físico subyacente. Por ejemplo, una máquina virtual se puede mover de un host físico a otro. Además, su disco virtual se puede mover de un tipo de almacenamiento a otro sin afectar el funcionamiento de la máquina virtual.

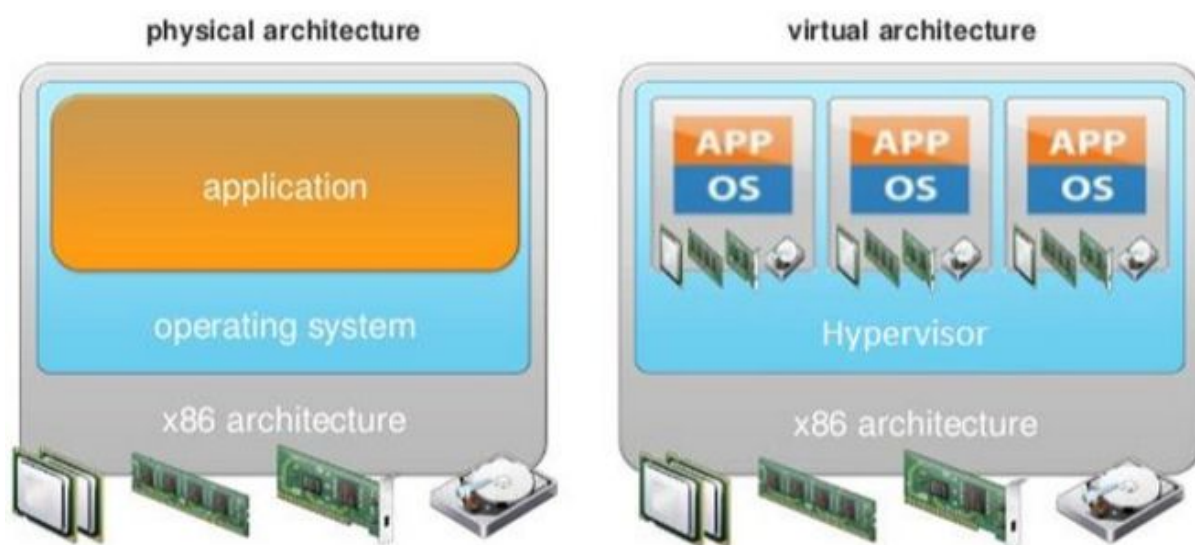


Figura 1:arquitectura física vs. virtual

## 2.3 Compartición de recursos

Un concepto clave para entender la virtualización es la noción de que los recursos físicos son compartidos. La virtualización permite ejecutar múltiples máquinas virtuales en una única máquina física, cada máquina virtual comparte los recursos de un equipo físico a través de múltiples entornos. Las máquinas virtuales comparten por ejemplo el acceso a la CPU, que es administrado por el Hipervisor. Además, las máquinas virtuales tienen su propia región de memoria disponible para utilizar y comparten el acceso a las tarjetas de red físicas y controladores de disco. Diferentes máquinas virtuales pueden ejecutar diferentes sistemas operativos y aplicaciones en el mismo equipo físico.

Cuando varias máquinas virtuales se ejecutan en un host anfitrión, a cada máquina virtual se asigna una parte de los recursos físicos. El Hipervisor organiza las máquinas virtuales, al igual que un sistema operativo tradicional, asignando memoria y programando las

aplicaciones para que se ejecuten en varios CPUs. Además administra el uso de disco y el ancho de banda de la red. Sin embargo, las máquinas virtuales son administradas mediante mecanismos de control elaborado que permiten gestionar el acceso que tiene disponible cada máquina virtual. Con la configuración de asignación de recursos por defecto, todas las máquinas virtuales asociadas con el mismo host reciben una parte igual de los recursos disponibles.

### **2.3.1 Virtualización de CPU**

La virtualización de CPU enfatiza el rendimiento y se ejecuta directamente en la CPU disponible siempre que sea posible. Los recursos físicos subyacentes se utilizan siempre que sea posible y la capa de virtualización ejecuta instrucciones sólo cuando es necesario para hacer que las máquinas virtuales operen como si se ejecutasen directamente en una máquina física.

La virtualización de CPU no es una emulación. No hay que confundir la emulación con la virtualización. La diferencia es que con la emulación todas las operaciones se ejecutan en software por un emulador de software. Un emulador de software permite que los programas se ejecuten en un sistema informático con un comportamiento similar para el cual fueron escritos originalmente. El emulador hace esto mediante la emulación, o reproducción del comportamiento del equipo original mediante la aceptación de los mismos datos o insumos para lograr los mismos resultados. La emulación ofrece portabilidad y corre el software diseñado para una plataforma a través de varias plataformas, pero por lo general el rendimiento se ve afectado negativamente.

Cuando muchas máquinas virtuales se están ejecutando en un host, estas máquinas virtuales pueden competir por recursos de CPU. Cuando se produce una contención de CPU, el host donde se aloja el hipervisor reparte los procesadores físicos en porciones de tiempo a todas las máquinas virtuales para que cada una se ejecute como si tuviera un número determinado de procesadores virtuales.

### **2.3.2 Uso de memoria en host físicos y virtualizados**

En un entorno no virtualizado, el sistema operativo asume que posee toda la memoria física del servidor. Cuando se inicia una aplicación que utiliza las interfaces proporcionadas por el sistema operativo, las páginas de memoria virtual son asignadas o liberadas durante la ejecución. La memoria virtual es una técnica conocida utilizada en la mayoría de los sistemas operativos de propósito general, y casi todos los procesadores modernos tienen hardware para apoyarla. La memoria virtual crea un espacio de dirección virtual uniforme para aplicaciones y permite que el sistema operativo y hardware puedan manejar la traducción de direcciones entre el espacio de direcciones virtuales y el espacio de direcciones físicas. Esta técnica se adapta al entorno de ejecución para soportar grandes espacios de direcciones, la protección de procesos, mapeo de archivos y swapping<sup>8</sup> en sistemas de computación modernos.

En un entorno virtualizado, la capa de virtualización crea un espacio de memoria direccionable contigua para la máquina virtual cuando se inicia. El espacio de memoria asignada se configura cuando se crea la máquina virtual y tiene las mismas propiedades que el espacio de direcciones virtuales. Esta configuración permite que el hipervisor pueda ejecutar múltiples máquinas virtuales de forma simultánea al tiempo que protege la memoria de cada máquina virtual del acceso de las demás.

### **2.3.3 Networking en host físicos y virtuales**

Los componentes de red virtuales clave en las arquitecturas virtualizadas son los adaptadores Ethernet virtuales y switches virtuales. Una máquina virtual puede ser configurada con uno o más adaptadores Ethernet virtuales. Los switches virtuales permiten que las máquinas virtuales en el mismo host anfitrión se comuniquen entre sí utilizando los mismos protocolos que utilizarían si las placas fueran físicas, sin necesidad de hardware adicional. Los switches virtuales soportan VLAN<sup>9</sup> y son compatibles con implementaciones estándar de VLAN de proveedores, como Cisco, HP, etc.

---

<sup>8</sup> Swapping es mover un proceso o parte de él temporalmente desde la memoria principal a un dispositivo secundario de almacenamiento (memoria de apoyo) para luego devolverlo a la memoria principal.

<sup>9</sup> VLAN, por sus siglas en inglés: Virtual Local Access Network.



El switch virtual se conecta a la red externa a través de adaptadores Ethernet salientes. El switch virtual es capaz de unir múltiples NIC<sup>10</sup> virtuales, de forma similar a un grupo de tarjetas de interfaz de red de un servidor tradicional, ofreciendo mayor disponibilidad y ancho de banda para las máquinas virtuales utilizando el switch virtual.

Los switches virtuales son similares a los switches físicos en muchos aspectos. Al igual que un switch físico, cada switch virtual está aislado y tiene su propia tabla de reenvío. Esta característica mejora la seguridad, haciendo más difícil para los hackers romper el aislamiento del switch virtual. También soportan segmentación de VLAN al nivel de puerto, de modo que cada puerto se puede configurar como un puerto de acceso o enlace troncal.

### **3. Etapa 1: Infraestructura de virtualización**

#### **3.1. Análisis de requerimientos de hardware de las aplicaciones**

La implementación práctica se realizará sobre un conjunto de aplicaciones solicitado por el Departamento de Sistemas, en función de los requerimientos de los docentes de las cátedras de la carrera de Ingeniería en Sistemas de Información.

Es preciso realizar un análisis de los requerimientos de hardware de cada uno de los software del conjunto y de la cantidad de equipos cliente que se espera puedan hacer uso de ellos en forma simultánea para poder dimensionar los recursos necesarios para ello.

En nuestro caso, el laboratorio de sistemas destinó un conjunto de 15 notebooks para que los alumnos hagan uso de las aplicaciones de laboratorio, por lo que tomamos como referencia este número a la hora de dimensionar los recursos de hardware del clúster de procesamiento según explicaremos en los siguientes capítulos.

A continuación se presentan los software y sus requerimientos de hardware:

---

<sup>10</sup> NIC, por sus siglas en inglés: Network Interface Card.

Software	Descripción	Procesador	Memoria	Disco	Licencia
AutoCad 2015	Software de diseño asistido por computadora	AMD o Intel 1 GHZ	2 GB	4 GB	Propietaria multiusuario
Matlab R2012A	Sistema de cómputo numérico	AMD o Intel	1 GB	3 GB	Propietaria multiusuario
Office Pro Plus 2016	Conjunto de herramientas de ofimática	AMD o Intel 1 GHZ	2 GB	3 GB	Licencia propietaria
Visio 2013	Software de dibujo vectorial	AMD o Intel 1 GHZ	2 GB	2 GB	Licencia propietaria
NetBeans IDE 8.2	Entorno de desarrollo integrado	AMD o Intel 800 MHZ	512 MB	750 MB	GPLv2
pgAdmin 4 (v 1.3)	Plataforma de administración y desarrollo para PostgreSQL	N/D	N/D	500 MB	Libre bajo PostgreSQL
Dr Racket v6.8	Lenguaje de programación de propósito general	N/D	N/D	450 MB	LGPL
Simio 6.106.11306	Simulador	AMD o Intel 1 GHZ	1 GB	500 MB	Propietaria multiusuario
Zinjal 20130801	IDE para C/C++	N/D	N/D	200 MB	GPLv2
Pharo 5.0	Lenguaje de programación orientado a objetos	N/D	N/D	100 MB	Libre bajo MIT license
Vensim PLE 5.10e	Software de simulación de fuerza industrial	N/D	N/D	4 MB	Libre versión educativa
PSeInt 20150920	Software de programación en pseudocódigo	N/D	N/D	30 MB	GPL
QtSpim 9.1.18	Emulador MIPS	N/D	N/D	75 MB	Libre bajo BSD license

Acrobat Reader DC 2017.012.20098	Lector de PDF	AMD o Intel 1.5 GHZ	1 GB	380 MB	Libre
SWI-Prolog 7.4.1	Interprete Prolog	N/D	N/D	70 MB	Libre bajo BSD license
NetLogo 6.0.1	Entorno de modelado	N/D	N/D	500 MB	GPL
Logisim 2.7.1	Simulador lógico	N/D	N/D	8 MB	GPL

Tabla 1: requerimientos de hardware de las aplicaciones

## 3.2. Estudio y elección de plataforma de procesamiento virtualizado

En este capítulo se presenta brevemente el estudio de tres plataformas de virtualización (Xenserver, Hyper-V, Proxmox) que se analizaron comparativamente para luego elegir la que se usó en la creación del clúster de procesamiento virtualizado.

### 3.2.1. Citrix Xenserver

Citrix XenServer es una plataforma de virtualización de nube, servidores y escritorios, Open Source y gratuita, desarrollada en conjunto por una comunidad (proyecto Xen) y por Citrix. De esta manera las empresas de cualquier tamaño tienen a su disposición esta potente solución a su alcance. Además cuenta con certificaciones de compatibilidad de hardware y ciclos de vida, dado que es producto comercial en el sentido de que se puede contratar un soporte con Citrix (Citrix Premier Support 24 x 7), y esto permite también la instalación automatizada desde la consola de administración Xencenter de las actualizaciones y upgrades publicadas.

El proyecto Xen desarrolla el Hypervisor Xen, open source. Tiene 10 años de desarrollo, lo que brinda una gran solidez. Es parte de la Linux Foundation y tiene licencia GPLv2<sup>11</sup>.

---

<sup>11</sup> GPLv2, por sus siglas en inglés: General Public License version 2, es una licencia de derecho de autor ampliamente usada en el mundo del software libre y código abierto, y garantiza a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir (copiar) y modificar el software.

Este hypervisor es utilizado por XenServer como el núcleo de su arquitectura, a la que Citrix añade otros componentes propios y XenCenter, la consola de administración.

## Arquitectura

Una infraestructura básica de XenServer se compone, similarmente a los demás entornos de virtualización corporativa más importantes (VMWare vSphere y Microsoft Hyper-V), de hosts físicos con el hypervisor instalado (XenServer) que proporcionan los recursos de microprocesador y memoria RAM<sup>12</sup> a las máquinas virtuales, una interfaz de administración (XenCenter, principalmente, o los comandos xe) y un recurso de almacenamiento local o remoto (SAN<sup>13</sup>, NAS<sup>14</sup>) en el que se encuentran alojadas las máquinas virtuales.

Las diferentes máquinas virtuales que se ejecutan en una máquina reciben el nombre de dominios en la terminología Xen. Existe un dominio privilegiado que es sobre el que se instala el “hipervisor” de Xen. Este dominio privilegiado recibe el nombre de dom0 y el resto de dominios reciben el nombre genérico de domU.



Figura 2: Arquitectura Xenserver

<sup>12</sup> RAM, por sus siglas en inglés: Random Access Memory

<sup>13</sup> SAN, por sus siglas en inglés: Storage Area Network.

<sup>14</sup> NAS, por sus siglas en inglés: Network Attached Storage.

### 3.2.2. Microsoft Hyper-V

Hyper-V es la plataforma de virtualización de servidores desarrollada por Microsoft. El rol Hyper-V permite crear y administrar un entorno virtualizado mediante la tecnología de virtualización integrada en Windows Server. Al instalar el rol Hyper-V, se instalan los componentes necesarios y, si lo desea, las herramientas de administración.

Los componentes necesarios incluyen el hipervisor de Windows, el servicio Administración de máquinas virtuales de Hyper-V, el proveedor de WMI de virtualización y otros componentes de virtualización, como el bus de máquina virtual (VMbus), el proveedor de servicios de virtualización (VSP) y el controlador de infraestructura virtual (VID).

Las herramientas de administración del rol Hyper-V se componen de lo siguiente:

- Herramientas de administración basadas en la GUI<sup>15</sup>: Administrador de Hyper-V, complemento Microsoft Management Console (MMC) y Conexión a máquina virtual, que da acceso a la salida de vídeo de una máquina virtual para poder interactuar con esa máquina.
- Cmdlets específicos de Hyper-V para Windows PowerShell: Windows Server 2012 incluye un módulo de Hyper-V que proporciona acceso de línea de comandos a toda la funcionalidad disponible en la GUI, así como también a la funcionalidad no disponible en ella.

La tecnología Hyper-V virtualiza el hardware para proporcionar un entorno en el que sea posible ejecutar varios sistemas operativos al mismo tiempo en un equipo físico. Hyper-V permite crear y administrar máquinas virtuales y sus recursos. Cada máquina virtual es un equipo virtualizado y aislado que puede ejecutar su propio sistema operativo. Un sistema operativo que se ejecuta dentro de una máquina virtual se denomina sistema operativo invitado.

Hyper-V puede ser instalada de dos formas diferentes. Dependiendo de qué tipo de instalación escojamos, obtendremos una serie de ventajas e inconvenientes:

---

<sup>15</sup> GUI, por sus siglas en inglés: Graphical User Interface.

- Versión dedicada: Versión gratuita “Hyper-V Server” que contiene todas las funcionalidades de Hyper-V pero ningún derecho de licencias.
- Como un rol de Windows Server: Éste se activa sobre una instalación completa o parcial del sistema operativo Microsoft Windows Server, beneficiándose de las ventajas de licenciamiento que esto conlleva. De esta forma por ejemplo al usar Hyper-V como rol de un Windows Server Datacenter que se licencia por socket, todas las VMs que se monten tendrán los derechos de Windows Server incluidos.

### **Arquitectura**

Hyper-V implementa el aislamiento de las máquinas virtuales en términos de una partición. Una partición es una unidad lógica de aislamiento, con el apoyo del hipervisor, en el que cada sistema operativo invitado se ejecuta. Una instancia hipervisor tiene que tener por lo menos una partición padre, que ejecuta una versión compatible de Windows Server (2008 o posterior). La pila de virtualización se ejecuta en la partición principal y tiene acceso directo a los dispositivos de hardware. La partición padre luego crea las particiones que albergan como invitados Sistemas Operativos hijos. Una partición padre crea particiones secundarias mediante la API hiperllamada, que es la interfaz de programación de aplicaciones expuestas por Hyper-V. En la figura siguiente se presenta una descripción de la arquitectura de Hyper-V:

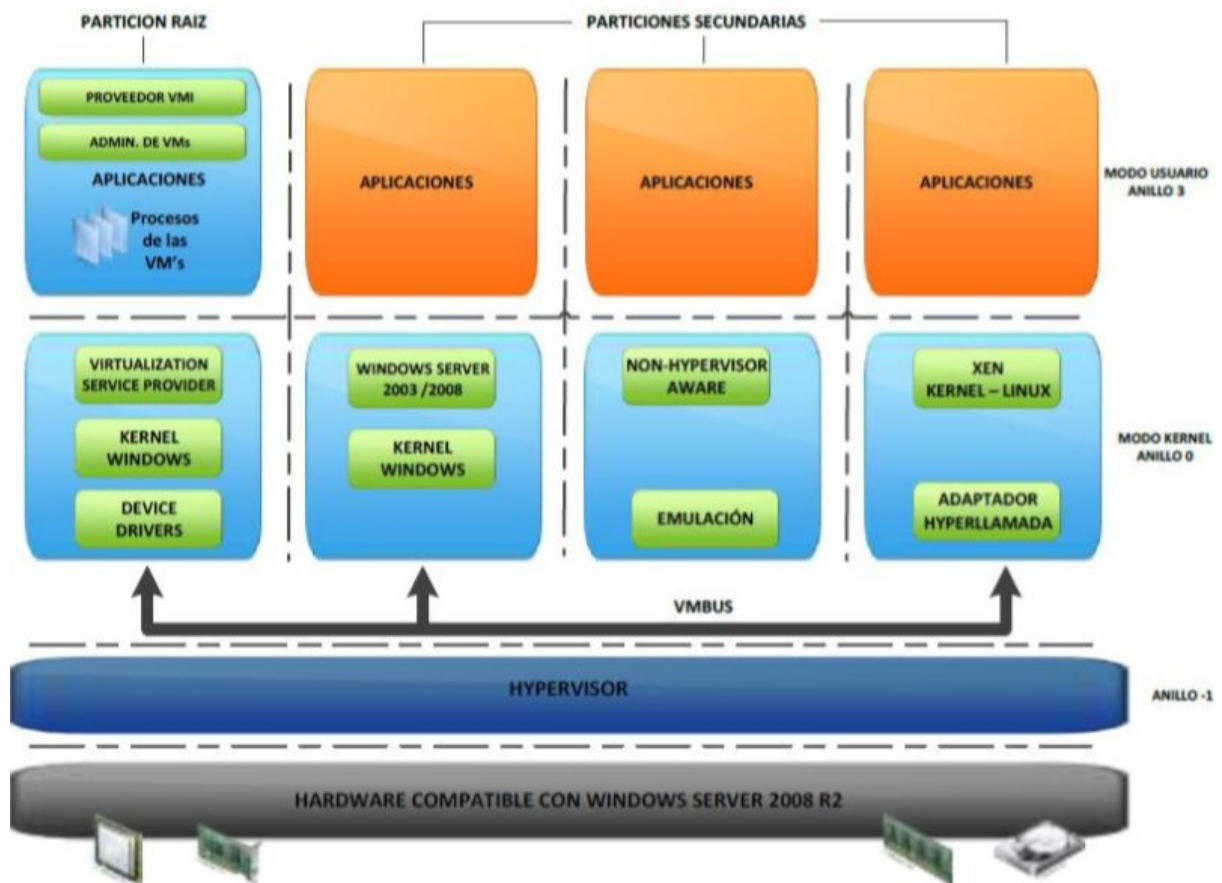


Figura 3: Arquitectura Hyper-V

Una partición hijo no tiene acceso al procesador físico, ni maneja sus interrupciones reales. En su lugar, tiene una vista virtual del procesador y corre en direcciones virtuales de invitado, que, dependiendo de la configuración del hipervisor, podría no ser necesariamente la totalidad del espacio de direcciones virtuales. Dependiendo de la configuración de la VM<sup>16</sup>, Hyper-V puede exponer sólo un subconjunto de los procesadores a cada partición. El hipervisor maneja las interrupciones al procesador, y las redirecciona a la respectiva partición utilizando un controlador de interrupción sintético lógico (synic).

Las particiones secundarias no tienen acceso directo a los recursos de hardware, sino que tienen una vista virtual de los recursos, en términos de dispositivos virtuales. Cualquier solicitud de los dispositivos virtuales se redirige a través del VMBus a los dispositivos en la partición principal, que gestionará las solicitudes. El VMBus es un canal lógico que permite la

<sup>16</sup> VM, por sus siglas en inglés: Virtual Machine.

comunicación entre particiones. La respuesta también es redirigida a través del VMBus. Si los dispositivos de la partición padre son también dispositivos virtuales, será redirigido hasta que alcance la partición principal, donde se tendrá acceso a los dispositivos físicos. Las particiones padre corren un Proveedor de Servicios de Virtualización (VSP), que conecta con el VMBus y maneja solicitudes de acceso del dispositivo de particiones secundarias. Los dispositivos virtuales de partición hijo ejecutan internamente un cliente de servicios de virtualización (VSC), que redirige la solicitud a VSP en la partición principal a través del VMBus. Todo este proceso es transparente para el sistema operativo invitado.

### **3.2.3. PROXMOX VE**

Proxmox VE es una plataforma completa de código abierto para la virtualización empresarial todo incluido que integra estrechamente el hipervisor KVM<sup>17</sup> y los contenedores LXC<sup>18</sup>, el almacenamiento definido por software y la funcionalidad de red en una sola plataforma, y administra fácilmente los clústeres de alta disponibilidad y las herramientas de recuperación de desastres con la interfaz de gestión web.

Las características de clase empresarial y el enfoque 100% basado en software hacen de Proxmox VE la opción perfecta para virtualizar su infraestructura de TI, optimizar los recursos existentes y aumentar la eficiencia con un costo mínimo. Permite virtualizar fácilmente incluso las cargas de trabajo de aplicaciones de Linux y Windows más exigentes, y escalar dinámicamente su computación y almacenamiento a medida que las necesidades crezcan, asegurándose de permanecer adaptable para el crecimiento futuro de un centro de datos.

#### **Arquitectura**

Proxmox es un Hypervisor de tipo 1 también conocido como nativo, unhosted o bare metal (sobre metal desnudo) por lo que el software de proxmox se ejecuta directamente sobre el hardware del equipo físico.

---

<sup>17</sup> KVM, por sus siglas en inglés: Kernel-based Virtual Machine. es una solución para implementar virtualización completa con Linux.

<sup>18</sup> LXC, Linux Containers: es una tecnología de virtualización en el nivel de sistema operativo para Linux. LXC no provee de una máquina virtual, más bien provee un entorno virtual que tiene su propio espacio de procesos y redes.



Proxmox es una solución completa de virtualización de servidores que implementa dos tecnologías de virtualización:

- KVM (Kernel-based Virtual Machine): Nos permite ejecutar múltiples VMs (Windows, Linux, Unix 32 o 64 bits), en la que cada VM tendrá su propio hardware virtual. KVM utiliza una versión modificada de QEMU, que es un emulador de procesadores con capacidad de virtualización (lo que hace QEMU es convertir el código binario de la arquitectura de la máquina física en código que pueda entender la VM huésped).
- LXC: Virtualización basada en contenedores para LINUX. Proxmox nos permite ejecutar múltiples “instancias” de sistemas operativos aislados sobre un único servidor físico, con la ventaja de que cada VM usa los recursos Hardware del servidor anfitrión, consiguiendo con esto mejoras en el rendimiento, escalabilidad, densidad, administración de recursos dinámico, etc. ya que cada VM se ejecuta sobre el propio Kernel del Servidor físico.

La siguiente figura presenta la arquitectura utilizada por Proxmox VE:

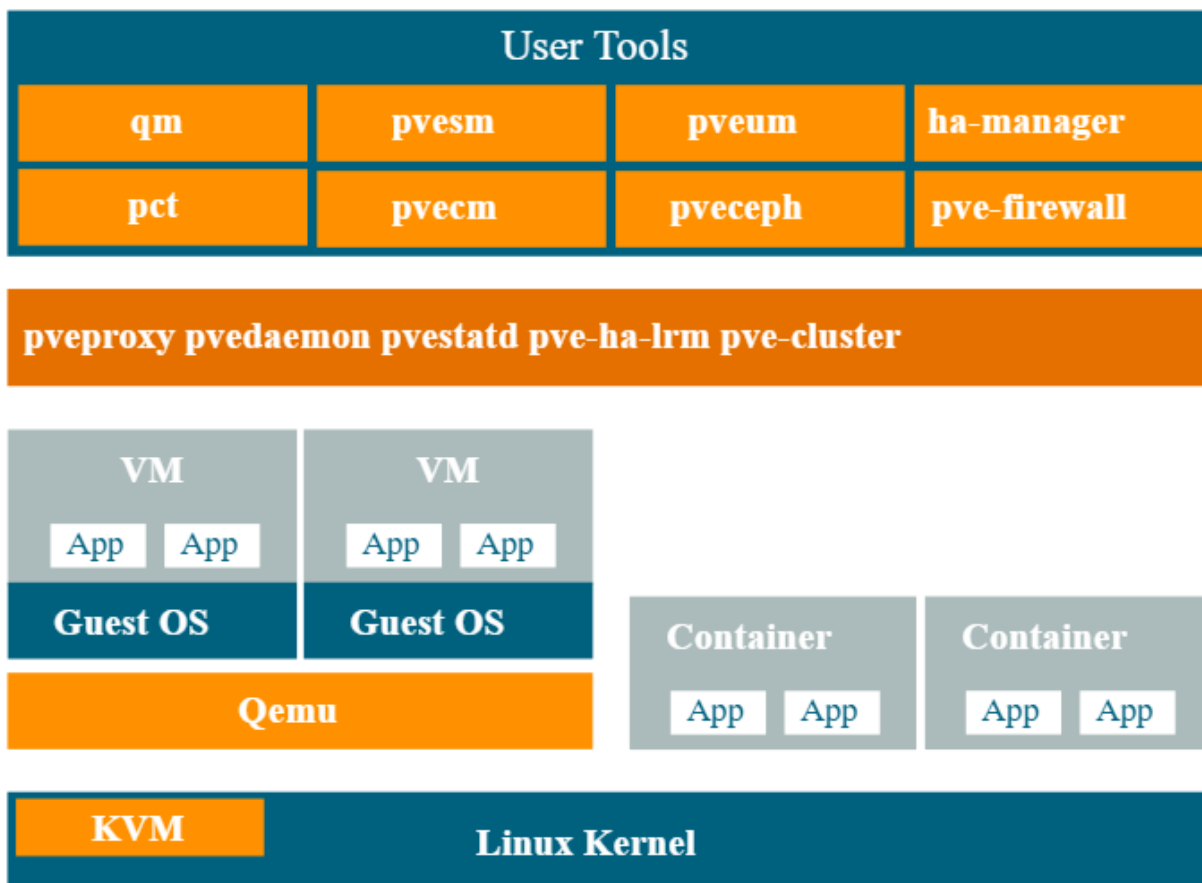


Figura 4: Arquitectura Proxmox VE

### 3.2.4. Comparación de las diversas herramientas

#### Ventajas de Xenserver

Xen es una plataforma de virtualización bajo licencia GPL que soporta arquitecturas del tipo x86, x86\_64 e ia64. Es capaz de ofrecer un rendimiento muy cercano al nativo en los dominios invitados y en aplicaciones, incluso para peticiones con grandes cargas de CPU y de entrada/salida de datos.

Posee un fuerte aislamiento entre dominios invitados. Esto permite un particionamiento completo entre dominios, lo que conlleva a mejorar la seguridad de la virtualización.

Cabe la posibilidad de salvar un estado y posteriormente restaurar dominios y la migración en caliente desde un servidor físico a otro manteniendo la disponibilidad total del dominio.

Posee extraordinaria escalabilidad a un gran número de dominios invitados, tales como: FreeBSD, NetBSD, Linux, Solaris, Windows (necesario hardware con tecnología Intel VT-x o AMD-V).

Soporta AGP<sup>19</sup>/DRM<sup>20</sup> en la parte gráfica y ACPI (Advanced Configuration and Power Interface) mejorado para la configuración avanzada de Energía.

### **Inconvenientes de Xenserver**

Xen comparte el mismo núcleo con el host, si se diera un fallo en el kernel este provocaría la caída de la totalidad de los servidores alojados.

Requiere de la instalación de un sistema operativo base y de su modificación post-instalación.

La curva de aprendizaje es un poco lenta si se está acostumbrado a trabajar con entornos gráficos.

El sistema operativo del host ha de ser única y exclusivamente FreeBSD, Linux o Solaris. Xen no soporta drivers propietarios de los entornos a emular.

### **Ventajas de Hyper-V**

Hyper-V Manager puede instalarse como un rol de Microsoft Windows Server R2 o bien directamente sobre un host limpio sin necesidad de un sistema operativo anfitrión.

Microsoft Windows Server R2 Hyper-V soporta procesadores físicos con más de ocho núcleos y hasta un total de sesenta y cuatro procesadores virtuales. En el apartado de memoria RAM es capaz de gestionar hasta 1TB<sup>21</sup> de memoria.

Hyper-V Manager posee una interfaz totalmente integrada con Microsoft Windows Server que proporciona una gestión intuitiva y una curva de aprendizaje muy poco pronunciada.

Hyper-V Manager, gracias a la característica Live Migration, es capaz de mover máquinas virtuales en caliente sin que el usuario note un cambio significativo en la conexión o similar a una caída del sistema o de la red. También permite el cambio de características del hardware

---

<sup>19</sup> AGP, por sus siglas en inglés, Accelerated Graphics Port.

<sup>20</sup> DRM, por sus siglas en inglés, Direct Rendering Manager.

<sup>21</sup> TB: TeraByte.

virtual de las máquinas virtuales en caliente sin tener que reiniciar para que los cambios se vean reflejados.

Hyper-V Manager permite hasta un total de cincuenta snapshots, otorgando una amplia flexibilidad y disponibilidad a la hora de recuperar en caso desastre.

No existe un número máximo (dependiendo de la versión de Hyper-V Manager) de instancias de máquinas virtuales y permite hasta 384 máquinas virtuales funcionando al mismo tiempo.

Hyper-V Manager dispone de aplicaciones ya integradas para la monitorización de máquinas virtuales.

### **Inconvenientes de Hyper-V**

A pesar de disponer de descarga gratuita, Hyper-V Manager funciona bajo licencia, por lo que si se quiere aplicar al ámbito profesional esta opción, se ha de tener en cuenta previo estudio económico, ya que dependiendo de la licencia contratada se obtendrá más o menos ventajas y características que potenciarán el uso de Hyper-V Manager en nuestro centro de datos.

Hyper-V Manager no es capaz de emular tarjetas de red inalámbricas ni tampoco es capaz de realizar un virtual switching sobre las mismas siendo estas físicas. Tampoco dispone de un centro de administración de redes centralizado, por lo que tendremos que mediar entre las configuraciones y opciones de Hyper-V Manager y las herramientas de Microsoft Windows Server.

Hyper-V Manager no soporta el port mirroring, esto hace que la administración de conexiones sea más compleja a la hora de permitir accesos de las máquinas virtuales a intranets o internet.

Los drivers utilizados para los dispositivos físicos son genéricos y no optimizados, por lo que se ve afectado el rendimiento. Esto conlleva que no se consigan resultados de rendimiento cercanos al de un hardware físico o nativo.

A pesar de poder migrar máquinas virtuales en caliente, no es posible migrar almacenamiento virtual en caliente.

No se dispone de un firewall integrado para aumentar la seguridad del sistema y de las máquinas virtuales.

La instalación es pesada, requiere un espacio superior a 3 GB<sup>22</sup> en disco incluso en su instalación desprendida de sistema operativo Microsoft Windows Server.

### **Ventajas de PROXMOX**

La solución de virtualización completa de máquina virtual basada en el kernel (KVM) es la técnica líder de virtualización de Linux. KVM es un módulo del kernel que se combina con el kernel de Linux principal y se ejecuta con un rendimiento casi nativo en todo el hardware x86 con soporte para virtualización, ya sea Intel VT-x o AMD-V.

PROXMOX proporciona un interfaz web para configurar los servidores físicos, cluster, máquinas virtuales, políticas de backups, restauración de backups, snapshots. No es necesario instalar aplicaciones clientes en su máquina para administrar.

En un "Cluster Proxmox" se debe definir uno de los Nodos como "Orquestador" con el objetivo de centralizar el trabajo, sin embargo cada nodo cuenta con su propio administrador web permitiendo acceso a la administración de las VMs. Si el nodo "Orquestador" llega a fallar, cada nodo tiene replicado la información del "Orquestador" y desde cualquiera de los nodos puede tomar control del cluster.

Container-based Virtualization (LXC), es una alternativa para ejecutar máquinas "Linux" en espacios separados. A diferencia de la virtualización este funciona como un módulo agregado al servidor físico y hace uso directo del hardware (también conocido como Paravirtualización).

En Proxmox el efectuar tareas de backup y restauración de máquinas virtuales es muy sencillo y se administra a través de su interfaz web. Puede efectuar un backup de forma inmediata o dejarlo programado. La restauración es simple, solo debe de seleccionar el backup a restaurar y el destino del almacenamiento de la copia.

---

<sup>22</sup>GB: GigaByte.

## Inconvenientes de PROXMOX

La funcionalidad de snapshot sobre VMs no está disponible sobre discos virtuales alojados en almacenamientos basados en LVM<sup>23</sup>.

Proxmox VE no permite administrar contenedores basados en Docker de forma nativa, sólo administra contenedores basados en LXC.

En lo que respecta a las configuraciones de networking, es necesario realizar y replicar en todos los nodos del cluster todas las configuraciones de red que se realicen. De este modo, por ejemplo, la incorporación de una subred al cluster debe configurarse en todos los nodos.

De modo similar a lo que ocurre con las configuraciones de networking, las conexiones a los dispositivos de almacenamiento en red como NAS o Storage también deben realizarse nodo a nodo.

## Tabla comparativa de Hipervisores

Presentamos en formato de tabla comparativa las principales características de los tres hipervisores estudiados:

Hipervisor	Citrix Xenserver	Microsoft Hyper-V	Proxmox VE
Compañía	Citric System Inc.	Microsoft Corp.	Proxmox Server Solutions Gmb
Posibles usuarios	Personal Small-Medium Business	Small-Medium Business	Small-Medium Business
Especificaciones técnicas			
Hypervisor tipo	1	1	1
Tipo de virtualización	Hardware Assisted Virtualization Paravirtualization	Full Virtualization Hardware Assisted Virtualization Operating System Virtualization	Full Virtualization Hardware Assisted Virtualization Paravirtualization Operating System Virtualization (LXC)

<sup>23</sup> LVM, por sus siglas en inglés: Logical Volume Manager. Es una implementación de un administrador de volúmenes lógicos para el kernel Linux.

Arquitectura	x86 x64	x86 x64	x86 x64
Almacenamiento Soportado	DAS <sup>24</sup> FC <sup>25</sup> iSCSI <sup>26</sup> NAS NFS <sup>27</sup> SAS SATA <sup>28</sup> USB <sup>29</sup>	DAS FC iSCSI SAS <sup>30</sup> SATA	DAS FC iSCSI SAS SATA NAS CEPH NFS GlusterFS Sheepdog CIFS <sup>31</sup>
Límites de Máquinas Virtuales			
Tamaño de disco virtual	2000 GB	2040 GB	GB
Memoria RAM	128 GB	64 GB	512 GB
CPUs virtuales (vCPU)	16	4	
Discos virtuales	16	256	
NICs virtuales	7	12	
Límites de Hosts			
Máquinas Virtuales	75 VMs	384 VMs	VMs
Memoria RAM	1024 GB	1024 GB	12 TB
Discos virtuales	512		

<sup>24</sup> DAS, por sus siglas en inglés: Direct Attached Storage.

<sup>25</sup> FC, por sus siglas en inglés: Fibre Channel.

<sup>26</sup> iSCSI, por sus siglas en inglés: internet Small Computer System Interface.

<sup>27</sup> NFS, por sus siglas en inglés: Network File System.

<sup>28</sup> SATA, por sus siglas en inglés: Serial Advanced Technology Attachment.

<sup>29</sup> USB, por sus siglas en inglés: Universal Serial Bus.

<sup>30</sup> SAS, por sus siglas en inglés: Serial Attached SCSI.

<sup>31</sup> CIFS, por sus siglas en inglés: Common Internet File System.

CPUs lógicos por host	160	64	768
CPUs virtuales por core		12	
Administración de virtualización			
Funcionalidades	Gestión de activos Configuration Mapping Snapshots Live Migration Reportes de performance Thin Provisioning Virtual Firewall	Capacity Planning/Management Dynamic Resource Allocation Real Time Alerts Shared Resource Pools	Dynamic Resource Allocation Live Migration P2V Conversion Performance Metrics Real Time Alerts Shared Resource Pools Storage Migration Thin Provisioning VM Backup/Restore VM Migration Virtual Firewall
Licencia	GNU GPL v2 y propietaria	propietaria	AGPL, v3

Tabla 2: comparativa Hipervisores

### Justificación de la elección

Analizando los pros y contras de cada alternativa estudiada concluimos que la elección más acertada es utilizar es PROXMOX VE.

Motiva esta elección la creciente popularidad de dicha herramienta en ambientes académicos y profesionales, debido principalmente a que no requiere de licenciamiento para su utilización y a que ofrece prácticamente las mismas funcionalidades que sus rivales. Una ventaja de esta herramienta en comparación a las restantes estudiadas es que posee una comunidad de usuarios en continuo crecimiento, lo que facilita la búsqueda e intercambio de información.

Vale aclarar que las restantes alternativas estudiadas no poseen características que las hacen inadecuadas para nuestra aplicación, pero requerirían costos de adquisición de licencias y/o de capacitación.



### **3.3. Análisis de requerimientos de hardware para clúster**

#### **3.3.1. Definición y estructura de un clúster**

Un clúster de computadoras se puede definir como un conjunto o conglomerado de computadoras, construidas con componentes de hardware comunes, que se comportan como una única computadora.

Un clúster es entonces un conjunto de computadoras, llamadas nodos, que están conectados entre sí a través de una red de cómputo de alta velocidad.

Cada nodo del clúster cuenta con varios procesadores y bancos de memoria, los cuales están interconectados entre sí. Los procesadores modernos son multinúcleo (o multi-core), cada núcleo es una unidad de procesamiento independiente. Esto es, cada procesador (chip, o encapsulado) contiene dos o más núcleos. La velocidad de acceso a la memoria en el clúster se acelera por medio de memoria llamada caché, la consistencia de los datos entre los procesadores, los bancos de memoria y la memoria caché se mantiene por medio de circuitos de coherencia de caché.

La red de comunicaciones entre los nodos juega un papel muy importante en la eficiencia del equipo. Un switch de red normal no es suficiente, se debe elegir un switch especializado considerando el gran volumen de datos y la velocidad con la que son requeridos. Es esencial realizar una buena selección del tipo de switch a utilizar a fin de garantizar un bajo tiempo de latencia (tiempo de espera al enviar datos de un nodo a otro) y capacidad de memoria intermedia para evitar congestión y pérdida de datos.

#### **3.3.2. Diseño del clúster**

Al diseñar el clúster se consideraron los siguientes aspectos:

**Economía y mantenimiento:** Utilización de componentes de bajo costo y además fácilmente reemplazables. Los componentes deben ser lo suficientemente comunes para poder ser reemplazados a un costo razonable en caso de fallo. Es importante incluir también el costo de mantenimiento y energía en el presupuesto destinado para el proyecto.

**Adecuación de las instalaciones:** Un clúster requiere de un ambiente controlado. Esto es, una habitación especial con sistema de enfriamiento, capacidad suficiente de carga eléctrica, control de humedad y un ambiente libre de polvo. Además se deben considerar el peso del equipo sobre el piso (ya sea falso o piso normal). Se recomienda colocarlo en los sótanos o en la planta baja de edificios.

**Escalabilidad:** Un clúster debe de ser escalable. Se recomienda seleccionar componentes de marcas reconocidas que soporten alta carga de trabajo de forma continua. Si se cuenta con un presupuesto bajo, pero se piensa crecer en un futuro, es importante seleccionar hardware al que se le pueda incrementar la cantidad de memoria, la capacidad de los procesadores y la capacidad de almacenamiento. Se debe llegar a un punto intermedio entre comprar hardware moderno y costoso y hardware antiguo de precio bajo que se vuelva obsoleto rápidamente.

**Interconexión:** Se debe considerar también el tipo de cableado a utilizar para conectar los nodos. Estos van desde cable UTP<sup>32</sup> de cobre hasta fibra óptica. Con respecto al switch, se deben tener en cuenta el tráfico que debe manejar según su función en la arquitectura del clúster.

**Almacenamiento:** es primordial contar con un espacio de almacenamiento compartido entre todos los nodos del clúster. Esto puede ser mediante un storage dedicado o mediante un NAS por software. Otro esquema posible es una solución de almacenamiento convergente, que abstrae los recursos de almacenamiento de los servidores que forman parte de una infraestructura virtual, utilizando los discos de dichos servidores para crear una capa de almacenamiento resistente y de alta performance, en la capa del Hipervisor. Ejemplos de estas soluciones son vSAN de VMWare y CEPH.

**Recursos humanos especializados:** Para garantizar el buen funcionamiento de un clúster se requiere contar con técnicos altamente especializados y actualizados en tecnologías de la información que puedan estar disponibles en la construcción y operación del mismo, a fin de sintonizar de forma efectiva el funcionamiento del equipo, así como modificaciones, actualizaciones y cuidado del mismo.

---

<sup>32</sup> UTP, por sus siglas en inglés: Unshielded Twisted Pair.

## 3.4. Diseño de clúster de procesamiento en alta disponibilidad

### 3.4.1. Arquitectura del Clúster

Nuestro diseño propuesto de clúster responde al protocolo de diseño de sistema en Alta Disponibilidad, cuya implementación asociada asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado. Disponibilidad se refiere a la habilidad de la comunidad de usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos. Si un usuario no puede acceder al sistema se dice que está no disponible. El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible.

Típicamente **tiempo de inactividad planificado** es el resultado del mantenimiento que resulta perjudicial para la operación del sistema y usualmente no puede ser evitado con la configuración actualmente instalada. Eventos que generan tiempos de inactividad planificados quizás incluyen parches al software del sistema que requieren un reinicio o cambios en la configuración del sistema que toman efecto después de un reinicio. En general el tiempo de inactividad planificado es usualmente el resultado de un evento lógico o de gestión iniciado.

**Tiempos de inactividad no planificado** surgen de algún evento físico tales como fallos en el hardware o anomalías ambientales. Ejemplos de eventos con tiempos de inactividad no planificados incluyen fallos de potencia, fallos en los componentes de CPU o RAM, una caída por recalentamiento, una ruptura lógica o física en las conexiones de red, rupturas de seguridad catastróficas o fallos en el sistema operativo o aplicaciones.

Para asegurar cierto grado de disponibilidad recurrimos a la **redundancia de hardware**. La redundancia hace referencia a nodos completos que están replicados o componentes de éstos, así como caminos u otros elementos de la red que están repetidos y que una de sus funciones principales es ser utilizados en caso de que haya una caída del sistema.

Concretamente, el diseño propuesto se compone de dos servidores, cuatro switches y un storage. La redundancia de servidores nos permite seguir procesando las máquinas virtuales ante la baja del servicio programada o accidental de uno de los nodos por completo. Para hacer esto posible es necesario albergar las máquinas virtuales en un espacio de

almacenamiento común que en nuestro caso es el storage. Sumado a esto, la comunicación entre los servidores y el storage se hace por dos caminos redundantes a través de dos switches separados, de modo tal que siga existiendo la comunicación aún ante la baja de uno de los switches o de las interfaces de red de un nodo o storage.

En la gráfica siguiente presentamos la topología física de la arquitectura propuesta.

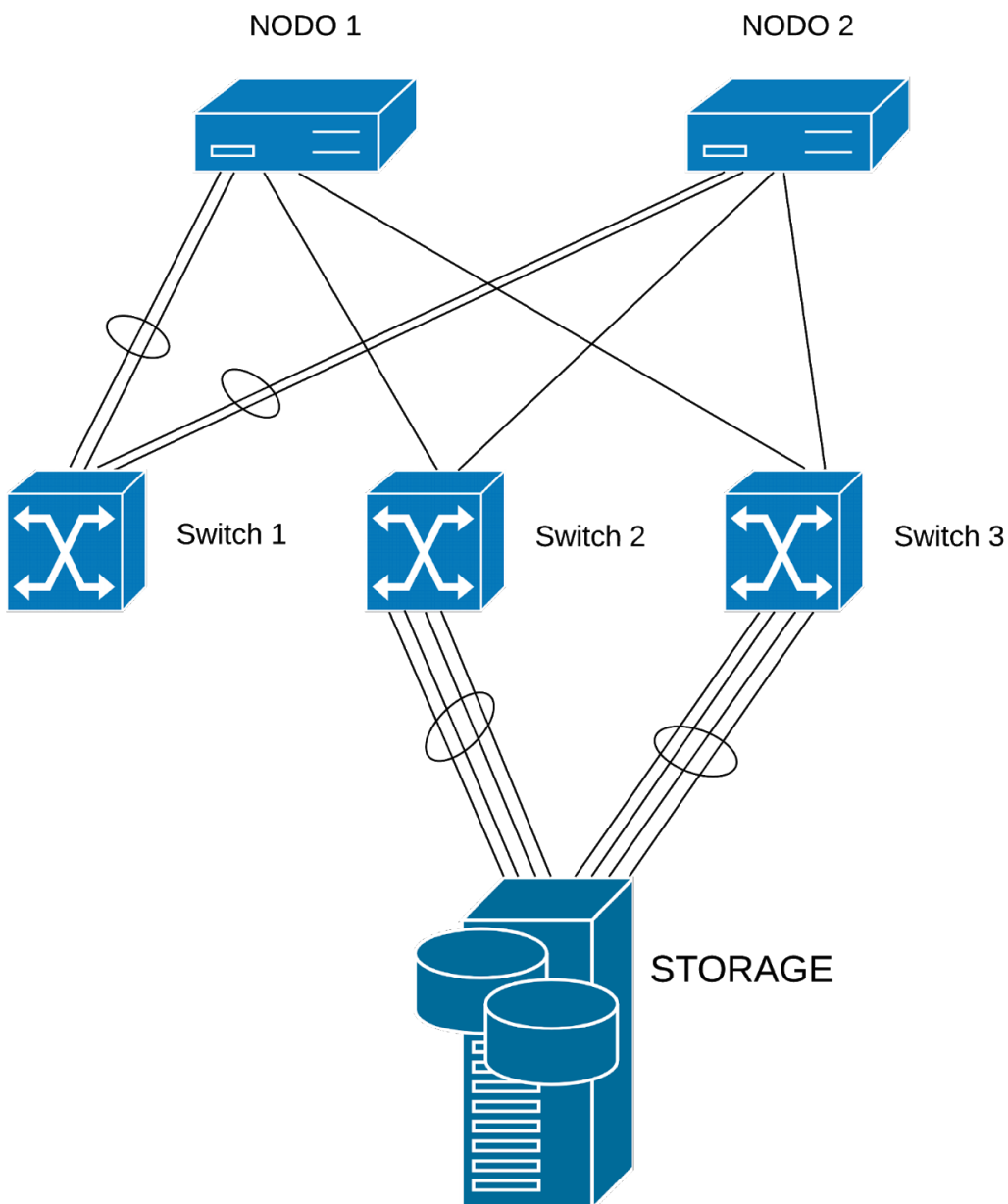


Figura 5: Topología física de Clúster.

Cada switch presente en la topología tiene una función específica:

- Switch de Intranet (switch 1): se emplea para la administración del clúster y para dar acceso a las máquinas virtuales a la red de producción.
- Switch de iSCSI (switch 2 y 3): estos switch componen la red de área de almacenamiento (SAN), para permitir la comunicación del área de almacenamiento (Storage), con los nodos del clúster. Es una red de alta velocidad totalmente aislada de la red de administración y producción.

### **3.4.2. Hardware empleado**

A continuación se detallan las características técnicas del hardware empleado en la construcción del clúster:

- Servidores:
  - Nodo 1 y 2:
    - Placa madre: Gigabyte GA-Z270-Gaming 3
    - Microprocesador: Intel(R) Core(TM) i7-7700
    - Memoria RAM: 4 x 16 GB DDR4 2666 MHZ Crucial Ballistix Sport LT
    - Tarjetas de red: 1 x onboard Killer™ E2500 LAN chip (10/100/1000 Mbit). 3 x TP-LINK TG-3468 PCI-E [Realtek RTL8111/8168/8411 (rev 06)]
    - Disco duro: WD Blue 1TB Desktop Hard Disk Drive - 7200 RPM SATA 6Gb/s 64MB Cache 3.5 Inch - WD10EZEX
    - Fuente de alimentación: Shure SH-600. 600 Watts.
    - Chasis: 4U rackeable genérico
- Switches:
  - Switch 1: HPE V1910-24G Switch
  - Switch 2: DELL PowerConnect 6224
  - Switch 3: 3Com Switch 4200G 24-Port
- Almacenamiento:

- Storage: HP P2000 G3 iSCSI

### 3.5. Implementación de infraestructura de cluster de servidores

En la sección Anexos se presentan los pasos empleados para la instalación y configuración de los Servidores y equipos de red y almacenamiento.

En esta sección nos limitaremos a presentar el diseño del direccionamiento de red del clúster.

La siguiente tabla presentan las direcciones ip asignadas a cada dispositivo presente en la topología del clúster.

Servicio	Dispositivo	Intranet		iSCSI			
		IP	switch1	IP1	switch 2	IP2	switch 3
Cluster	Nodo1	10.1.4.10	1,2	10.5.20.10	5	10.5.10.10	5
	Nodo2	10.1.4.20	3,4	10.5.20.20	6	10.5.10.20	6
Storage	ISCSI Storage 1 - 1					10.5.10.1	1
	ISCSI Storage 1 - 2					10.5.10.2	2
	ISCSI Storage 1 - 3			10.5.20.1	1		
	ISCSI Storage 1 - 4			10.5.20.2	2		
	ISCSI Storage 2 - 1					10.5.10.3	3
	ISCSI Storage 2 - 2					10.5.10.4	4
	ISCSI Storage 2 - 3			10.5.20.3	3		
	ISCSI Storage 2 - 4			10.5.20.4	4		
Administración	Administracion Storage 1 - 1	10.4.80.1					
	Administracion Storage 1 - 2	10.4.80.2					
	switch1	10.4.10.1	INTRANET				
	switch2	10.4.10.2	iSCSI				
	switch3	10.4.10.3	iSCSI				

Tabla 3: Direccionamiento IP de Clúster

A continuación se presenta un diagrama de topología lógica de la red:

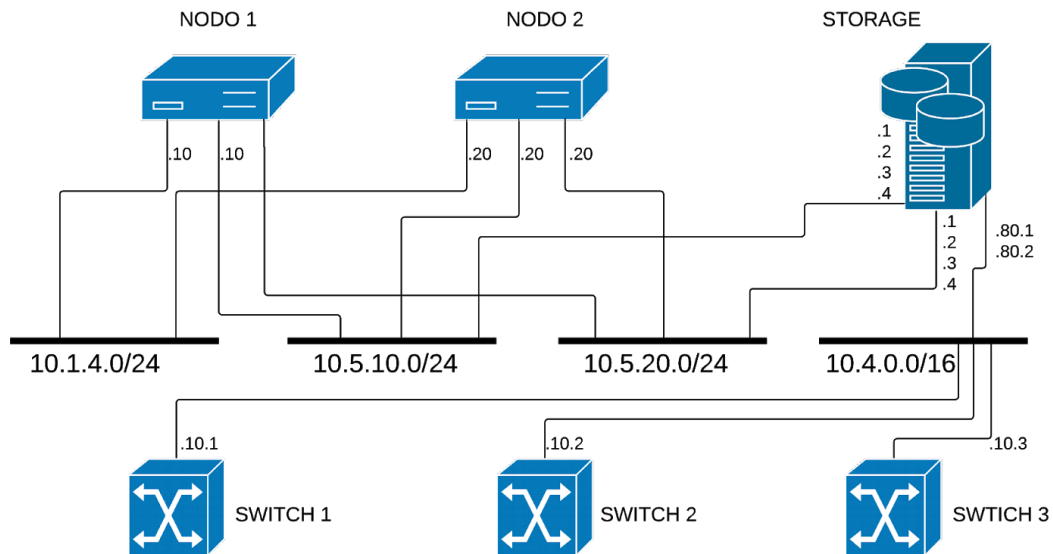


Figura 6: Topología lógica del Clúster

## 4. Etapa 2: Sistemas Operativos y colecciones de software

### 4.1. Análisis, diseño e implementación de arquitectura de procesamiento remoto

Partiendo de la base de un clúster de servidores para procesamiento, comenzaremos el análisis de alternativas para la implementación de la arquitectura de virtualización de aplicaciones.

Existen algunas soluciones de software en el mercado para la virtualización de aplicaciones de escritorio. Entre las principales se encuentran VMWare Horizon, Citrix Xenapp y Microsoft RDS. Las características de estas soluciones son muy similares y para nuestra aplicación específica es posible emplear cualquiera de ellas. Las soluciones mencionadas requieren licencia propietaria para su utilización, por lo que en este caso nuestra elección estuvo influida por el hecho de que en la UTN se dispone de un convenio con

Microsoft por el cual disponemos de acceso licenciado a muchos productos de la marca, incluidos los necesarios para utilizar Microsoft RDS, motivo por el cual fue nuestra elección.

#### 4.1.1. Arquitectura de Virtualización de Aplicaciones

Microsoft RDS (Remote Desktop Service) es un software de virtualización de aplicaciones que entrega aplicaciones de Windows alojadas centralmente a dispositivos locales sin la necesidad de instalarlas.

Para tener una idea de la capacidad de RDS, resulta esencial comprender las funciones de sus componentes principales de la arquitectura, a la vez de cómo interactúan entre sí para procesar un requerimiento de RDS. Existe una nueva terminología y acrónimos con los cuáles debemos familiarizarnos dentro del contexto de RDS.

Existen cinco roles primordiales dentro de la Arquitectura de RDS, como se puede observar en la imagen siguiente, y todos requieren de un servidor de licenciamiento **Remote Desktop Licensing (RDL)**. Cada componente incluye un conjunto de características diseñadas para adquirir ciertas funciones específicas dentro de la Arquitectura RDS.

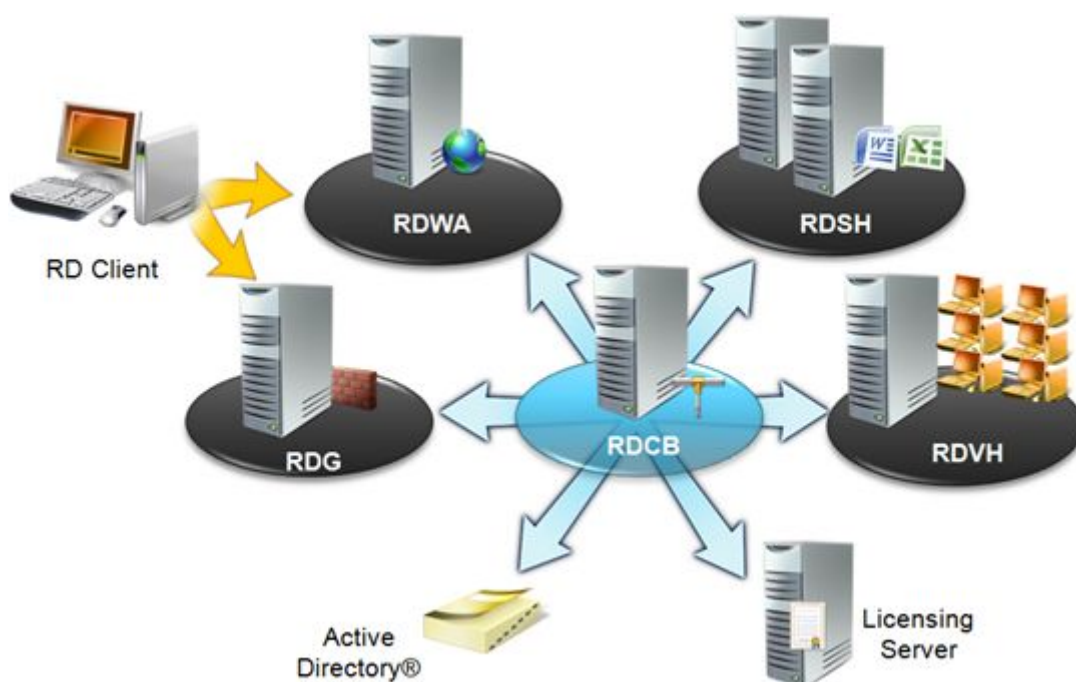


Figura 7: Arquitectura RDS



Para comenzar, un usuario final deberá acceder a la URL<sup>33</sup> de RDS, la cuál será la URL que contenga los recursos publicados (aplicaciones). La interface, provista por **Remote Desktop Web Access (RDWA)**, y configurada a través de un **Internet Information Services (IIS)** con SSL, es el punto de acceso Web para RemoteApp. La URL de acceso, es consistente independientemente de cómo los recursos son organizados, compuestos, y publicados desde múltiples servidores de sesión RDS por detrás. Por defecto, RDS publica los recursos en el siguiente formato de URL `https://FQDN-del-Webaccess-server-RDWA/rdweb` y esta URL es la única información que el administrador deberá proveer a los usuarios finales, para acceder a los recursos autorizados a través de RDS. Un usuario final necesitará autenticarse con sus credenciales de **Active Directory (AD)** cuando acceda a la URL del **RDWA**, haciendo que las aplicaciones y recursos publicados sean "presentados" al usuario final en base a los permisos otorgados en la lista de control de accesos. Es decir, el usuario final solo podrá ver y acceder aquellos recursos a los cuáles su cuenta de **AD** posea permiso.

**Remote Desktop Gateway (RDG)** es opcional y se ubica en el borde de la red corporativa para filtrar los requerimientos externos de RDS, en base al criterio de acceso definido en un servidor llamado **Network Policy Server (NPS)**. Basado en certificados, **RDG** ofrece acceso remoto seguro hacia la infraestructura de RDS. Para el administrador de sistemas, el **RDG** es la frontera de una red de RDS. En nuestra aplicación no utilizamos esta funcionalidad.

En RDS, las aplicaciones son instaladas y publicadas en un **Remote Desktop Session Host (RDSH)**. Un **RDSH** carga las aplicaciones, las ejecuta, y muestra los resultados. El "Sign-in Digital" puede ser fácilmente habilitado en un **RDSH** con un certificado. Múltiples **RDSH** pueden ser configurados con tecnología de "balanceo de carga". Esto requiere que cada **RDSH** en un grupo de balanceo de carga necesite ser configurado idéntico de la misma manera, y con exactamente las mismas aplicaciones.

**Remote Desktop Virtualization Host (RDVH)** es una característica que atiende los requerimientos para escritorios virtuales ejecutándose en máquinas virtuales, o asignación de máquinas virtuales en sí. Un servidor **RDVH** se encuentra basado en Hyper-V, por ejemplo

---

<sup>33</sup> URL, por sus siglas en inglés: Uniform Resource Locator.

un servidor Windows con el rol de Hyper-V habilitado. Al momento de atender un requerimiento de usuario con necesidad de asignación de una VM, un servidor **RDVH** automáticamente iniciará una VM, en el caso que la misma ya no se encuentre ejecutándose. Paso siguiente, el usuario final requerirá colocar sus credenciales al ingresar al escritorio virtual. Sin embargo, un **RDVH** no acepta de manera directa los requerimientos de conexión, utiliza en cambio un **RDSH** como "redirector" para atender los requerimientos basados en VMs. El par de un **RDVH** junto con su "redirector", es definido dentro del **Remote Desktop Connection Broker (RDCB)** al momento de agregarse un recurso basado en **RDVH**. Para nuestra aplicación práctica no haremos uso de las funciones de **RDVH**.

**Remote Desktop Connection Broker (RDCB)**, proporciona una experiencia unificada para configurar el acceso de los usuarios a las aplicaciones tradicionales y a los escritorios virtuales basados en máquinas virtuales. Aquí, un escritorio virtual puede estar ejecutándose tanto en una VM designada, o una VM dinámicamente asignada, basándose en la carga de balanceo, desde un "pool" definido de VMs. Un administrador de sistemas utilizará la consola de **RDCB**, llamada **Remote Desktop Connection Manager**, para agregar **RDSHs** y **RDVHs**, como así también aquellas aplicaciones publicadas por los **RDSHs**. De la misma manera, aquellas VMs ejecutándose en los **RDVHs**, podrán ser publicadas luego a través de la URL del **RDWA**. Una vez autenticados los usuarios finales en esta URL del **RDWA**, los usuarios podrán acceder a las aplicaciones autorizadas (RemoteApp), y escritorios virtuales.

Un cliente de **Remote Desktop (RD)** obtiene información de la conexión a realizar desde el servidor **RDWA** dentro de una estructura de RDS. Si el cliente **RD** se encuentra por fuera de la red corporativa, el cliente se conectará a través del **RDG**. En cambio si el cliente **RD** se encuentra dentro de la red corporativa, el cliente podrá luego conectarse de manera directa tanto hacia un **RDSH**, como también hacia un **RDVH**, toda vez que el **RDCB** provea la información de la conexión. En ambos casos, el **RDCB** juega un papel primordial a la hora de proveer al cliente **RD**, el acceso al recurso apropiado. Mediante el uso de certificados, el administrador de red puede configurar el **Single Sign ON (SSO)** entre los varios componentes de RDS, para proveer al usuario final una experiencia confortable y segura.

Conceptualmente, el **RDCB** es el "jefe de operaciones" dentro de una **Arquitectura de RDS**, y sabe dónde está cada recurso, con quién contactarse, y qué realizar con cada petición

de RDS. Antes de que una conexión lógica pueda establecerse entre un cliente y un **RDSH** o **RDVH** de destino, el **RDCB** actúa como un "enlace", enviando la información pertinente "desde y hacia" los diferentes componentes, al momento de atender una petición de RDS.

#### **4.1.2. Diseño e implementación de RDS**

Habiendo estudiado la arquitectura de Microsoft RDS y poniéndola en contraste con las nuestros objetivos, podemos acotar los roles y prescindir de **Remote Desktop Gateway (RDG)** y de **Remote Desktop Virtualization Host (RDVH)**, debido a que en un principio nuestro alcance está limitado a la red LAN y a aplicaciones de escritorio.

Teniendo en cuenta lo anterior, proponemos un diseño de arquitectura compuesto por:

RDWA, RDL, RDCB, RDSH (dos servidores para permitir balanceo de carga) y AD.

Los roles de RDWA , RDCB y RDL estarán agrupados en una VM con sistema operativo Windows Server 2012 Standard. De igual modo, los roles de AD y Servidor de Licencias de Aplicaciones (ALS) (los cuales explicaremos en una sección posterior) estarán agrupados en una VM con Windows Server 2012 R2. Finalmente, se emplearán dos VMs con Windows Server 2012 Standard para los roles de RDSH, de modo de que la carga de procesamiento de las aplicaciones pueda distribuirse equitativamente entre ambos por medio del RDCB. En la figura siguiente se presenta la arquitectura de virtualización de aplicaciones propuesta.

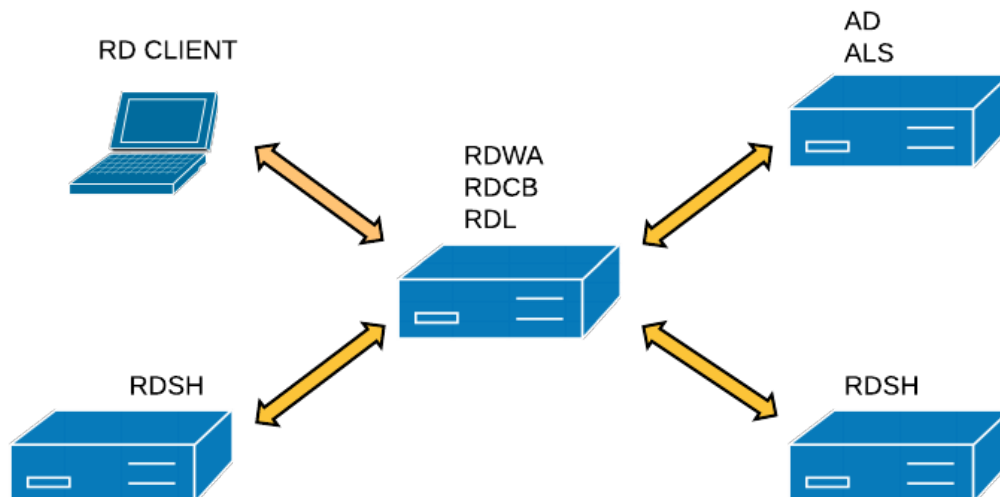


Figura 8: Arquitectura virtualización de aplicaciones.

En la sección Anexos se presentan los detalles de la implementación de los roles presentes en la arquitectura de virtualización de aplicaciones propuesta.

## 4.2. Creación de máquinas virtuales y colecciones de software

### 4.2.1. Los RDSHs

Como mencionamos anteriormente, la arquitectura de RDS propuesta está compuesta por dos servidores RDSH, los cuales serán los encargados de realizar el procesamiento de las aplicaciones de escritorio de forma centralizada. Cada RDSH es una VM con recursos suficientes para soportar la carga de procesamiento de 10 clientes remotos simultáneos aproximadamente, con lo cual se aseguran recursos para un total de 20 clientes simultáneos.

La configuración de estos servidores es sencilla, dado que sólo se encargan de procesar las aplicaciones y entregar los resultados a los clientes remotos. El sistema operativo base es Windows Server Standard con el rol RDS activado y con todas las aplicaciones de escritorio que se quieran publicar.

En la sección Anexos se presentan los pasos para la activación del rol RDS en Windows Server Standard.

#### **4.2.2. Las colecciones de software**

Una vez configurados los RDSH es necesario configurar el RDCB para administrar las peticiones que los clientes hacen a los RDSH. En nuestra arquitectura, un servidor RDCB se encargará de administrar las conexiones de los clientes RD hacia los RDSHs.

La configuración del RDCB involucra los siguientes aspectos:

- Activar rol RDCB
- Incorporar servidores RDSH a administrar
- Grupos/Usuarios permitidos
- Parámetros de las sesiones
- Seguridad
- Balanceo de carga
- Parámetros de los clientes
- Colecciones de softwares

En la sección Anexos presentamos el paso a paso de la configuración del RDCB.

### **4.3. Estudio e implementación de servidor de licencias flotantes**

#### **4.3.1. Servidor de licencias de escritorio remoto (RDL<sup>34</sup>)**

Cada usuario y dispositivo que se conecta a un RDSH necesita licencias de acceso de cliente (CAL<sup>35</sup>). Cuando un usuario o un dispositivo se conecta a un RDSH, el servidor determina si se necesita una CAL de RDS. El RDSH luego solicita una CAL de RDS del RDL. Si una CAL de RDS adecuada está disponible desde un RDL, la CAL de RDS se emite al cliente, y el cliente puede conectarse al RDSH y desde allí al escritorio o las aplicaciones que están tratando de usar.

---

<sup>34</sup> RDS, por sus siglas en inglés: Remote Desktop Licensing.

<sup>35</sup> CAL, por sus siglas en inglés: Client Access License.

En nuestra arquitectura, el rol de RDL se encuentra corriendo en el mismo servidor que el RDCB. Para nuestra aplicación sólo es preciso contar con una licencia para usuario CAL, dado que, como explicaremos en apartados posteriores, el acceso a las aplicaciones se hará con un único usuario de dominio dado que se permiten sesiones simultáneas. Cabe aclarar que la disponibilidad de la licencia para RDL por parte de la UTN está contemplada dentro del convenio existente con Microsoft.

En la sección Anexos se presenta el paso a paso de la implementación del rol RDL en Windows Server Standard.

#### **4.3.2. Servidor de licencias para aplicaciones (ALS<sup>36</sup>)**

Las diversas aplicaciones de la colección poseen diferentes tipos de licenciamiento para su uso (como se puede ver en la tabla 1). Haremos hincapié en las licencias de tipo multiusuario, debido a que son las que requieren un tratamiento especial para nuestra aplicación.

Las licencias de tipo **multiusuario o flotante** admiten un número máximo de usuarios específico en equipos conectados a una red. Las licencias se emiten mediante un servidor de administración de licencias de red (NLM<sup>37</sup>) para cada usuario que inicia un producto determinado, hasta el número de licencias adquiridas. Por lo general, la licencia se devuelve a NLM cuando un usuario cierra todos los productos, lo que hace que esté disponible para otros usuarios.

Los software para los servicios de NLM pueden ser propiedad de los editores de las aplicaciones o de terceras partes. En nuestra aplicación práctica tenemos tres software basados en esquema de licenciamiento multiusuario o flotante: AutoCad 2015, Matlab R2012A y Simio 6. De ellos, los 2 primeros poseen tipos de licencia que permiten su administración mediante el software NLM de FLEXERA mientras que para el tercero el editor del software posee un NLM propietario.

---

<sup>36</sup> ALS, por sus siglas en inglés: Application License Server.

<sup>37</sup> NLM, por sus siglas en inglés: Network License Manager.

#### 4.3.2.1. NLM Flexera

Flexnet Publisher es un método de provisión de licencias de software que tiene dos componentes básicos:

- Aplicaciones FlexEnabled: el software que requiere una licencia.
- Una licencia: contiene los derechos de licencia que definen cómo se puede usar la aplicación de software.

Normalmente una licencia define:

- Qué funcionalidades del software se pueden utilizar. Las funciones proporcionadas por el software se pueden licenciar por separado.

Las funciones licenciadas se conocen como características. Cuando se definen múltiples características, diferentes versiones del producto pueden ser licenciadas incluyendo diferentes conjuntos de características.

- Qué versión del software puede ser usado.
- Cuántas copias del software se pueden ejecutar.
- Los sistemas sobre los cuales el software se puede usar.
- El período durante el cual se puede usar el software.

Las licencias son archivos de texto, cuyo contenido está protegido por firmas autenticadas por los componentes de licencia de FlexNet Publisher.

Los componentes básicos de un servidor de licencias FlexNet Publisher incluyen:

- Administrador del servidor de licencias: ladmin (o lmgrd) proporcionado por el proveedor del software o disponible en Flexera.
- Archivo de Licencia: creado por el proveedor de software.
- Demonio del vendedor: demonio proporcionado por el proveedor del software.
- Debug log: escritos por el administrador del servidor de licencias.

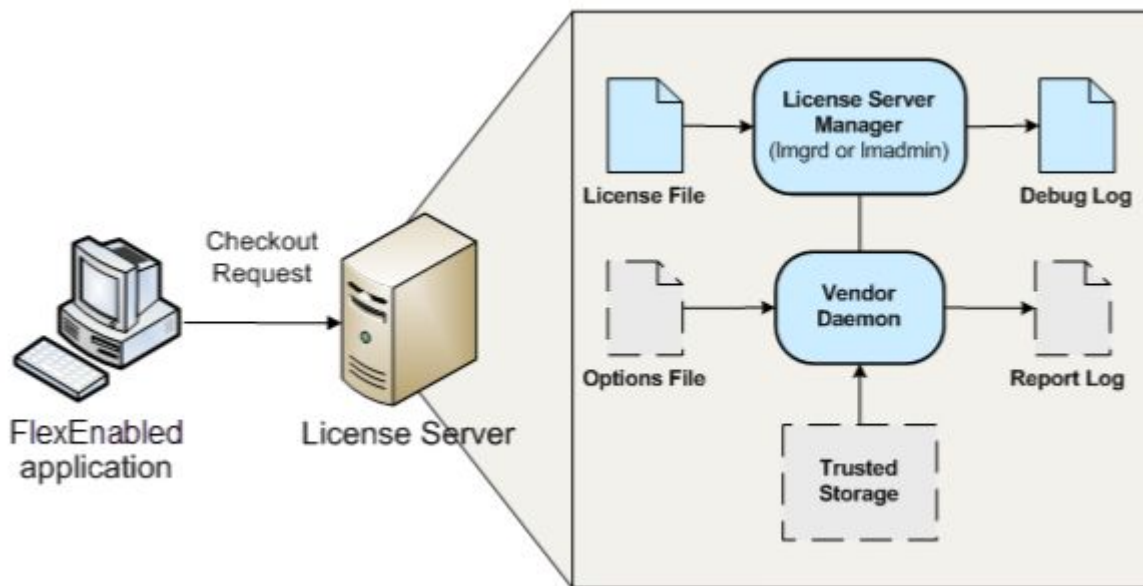


Figura 9: servidor de licencias FlexNet Publisher.

A continuación se ofrece un resumen de los pasos para instalar un servidor de licencias:

1. Elija las máquinas en las que se instalarán los servidores de licencias.
2. Instale los componentes del servidor de licencias.

El editor proporcionará una copia de su demonio de vendedor e instrucciones para instalarlo. Además, el editor proporciona el administrador del servidor de licencias (lmgrd), o puede descargar una copia del sitio web de Flexera Software.

3. Obtenga los detalles de la (s) máquina (s) del servidor de licencias y envíelos al editor. Normalmente, los editores suministran licencias concurrentes que están bloqueadas a un servidor de licencias específico. Cuando las licencias se guardan en archivos de licencia, se bloquean en el servidor de licencias utilizando una identidad obtenida de la máquina. Esta identidad se denomina hostid y es específica de la plataforma. Hay varios hostids diferentes disponibles para cada plataforma. El editor proporcionará instrucciones sobre qué hostid están utilizando para sus licencias y plataformas. Según el modelo de licencia, el editor puede requerir otros detalles de su servidor de licencias, la máquina en la que se está ejecutando y los detalles de su red.



4. Instale las licencias en el servidor de licencias.

El editor puede especificar una ubicación particular para los archivos de licencia en el servidor de licencias, aunque no siempre es requerido.

5. Instale la aplicaciones FlexEnabled (aplicaciones a licenciar) en las máquinas de los usuarios finales.

El editor proporcionará instrucciones de instalación para instalar la aplicación FlexEnabled.

6. Configure las máquinas de los usuarios finales para acceder al servidor de licencias.

Existen varios métodos para configurar la máquina del usuario final para acceder a un solo servidor de licencias o múltiples servidores de licencias. Estos dependen del contenido de los archivos de licencia suministrados por el editor y de la configuración de su servidor de licencias.

7. Opcionalmente, cree un archivo de opciones.

Si desea limitar el uso de la licencia, configurar el registro o desactivar la lectura automática de licencias, cree un archivo de opciones e instálelo en el mismo directorio que el daemon del proveedor.

8. Configure e inicie el administrador del servidor de licencias.

lmgrd: los ajustes de configuración se establecen cuando se inicia lmgrd. No son persistentes.

En la sección Anexos se presentan los pasos para la configuración del NLM Flexera.

#### **4.4. Diseño y creación de perfiles de acceso a los software (Active Directory)**

Como mencionamos en la sección 4.1.1.: “Un usuario final necesitará autenticarse con sus credenciales de **Active Directory (AD)** cuando acceda a la URL del **RDWA**, haciendo que las aplicaciones y recursos publicados sean "presentados" al usuario final en base a los permisos otorgados en la lista de control de accesos. Es decir, el usuario final solo podrá ver y acceder aquellos recursos a los cuáles su cuenta de AD posee el permiso requerido.”

El servidor de AD se implementó mediante una VM basada en Windows Server 2012 R2 con el correspondiente Rol de Active Directory instalado. En nuestro caso, la UTN FRSF disponía de un servidor Active Directory ya implementado, por lo que sólo fue necesario crear un usuario de dominio (denominado **Labmovil**) para permitir el acceso a la aplicaciones remotas.

En la sección Anexo se muestran los pasos para la activación del Rol y creación del usuario de dominio.

A continuación se presenta una breve descripción del Rol de Active Directory para una comprensión general.

#### **4.4.1. Active Directory**

Active Directory (AD) o Directorio Activo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadoras.

De forma sencilla se puede decir que es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

#### **4.4.1.1. Funcionamiento**

Su funcionamiento es similar a otras estructuras de LDAP<sup>38</sup>, ya que este protocolo viene implementado de forma similar a una base de datos, la cual almacena en forma centralizada toda la información relativa a un dominio de autenticación. Una de sus ventajas es la sincronización presente entre los distintos servidores de autenticación de todo el dominio.

A su vez, cada uno de estos objetos tendrá atributos que permiten identificarlos en modo unívoco (por ejemplo, los usuarios tendrán campo «nombre», campo «email», etcétera, las impresoras de red tendrán campo «nombre», campo «fabricante», campo «modelo», campo "usuarios que pueden acceder", etc). Toda esta información queda almacenada en Active Directory replicándose de forma automática entre todos los servidores que controlan el acceso al dominio.

De esta forma, es posible crear recursos (como carpetas compartidas, impresoras de red, etc) y conceder acceso a estos recursos a usuarios, con la ventaja que estando todos estos objetos memorizados en Active Directory, y siendo esta lista de objetos replicada a todo el dominio de administración, los eventuales cambios serán visibles en todo el ámbito. Para decirlo en otras palabras, Active Directory es una implementación de servicio de directorio centralizado en una red distribuida que facilita el control, la administración y la consulta de todos los elementos lógicos de una red (como pueden ser usuarios, equipos y recursos).

### **4.5. Diseño e implementación de seguridad en sistemas operativos (Firewall, Backups)**

Para el diseño de seguridad tomamos como base los servidores presentes en la arquitectura de virtualización de aplicaciones (figura 8). Podemos dividir el diseño de seguridad en dos apartados: control de acceso (firewall) y copias de respaldo (backups).

#### **4.5.1. Firewall**

A los efectos de brindar el servicio de virtualización de aplicaciones, los usuarios finales sólo precisarán acceder a los servidores RDSH, más precisamente al puerto que escucha

---

<sup>38</sup> LDAP, por sus siglas en inglés: Lightweight Directory Access Protocol.

peticiones de conexiones RDS (TCP<sup>39</sup>/UDP<sup>40</sup> 3389). Para esto, deberemos crear reglas de firewall de entrada para las redes deseadas (red de clientes y de administración) al puerto y protocolo en cuestión, de modo que los RDSH sólo acepten conexiones RDP desde las redes especificadas. Estas reglas de firewall se configuran directamente sobre el sistema operativo de los RDSH.

En el capítulo 5 se explica el diseño de las redes de clientes y servidores.

En la sección Anexos se muestra el paso a paso para la implementación de las reglas de firewall en Windows Server 2012 Standard.

#### **4.5.2. Backups**

A modo de respaldo ante catástrofe realizaremos backups de las máquinas virtuales completas. Las VMs a respaldar son tres (véase la figura 8): uno de los RDSH (dado que los dos son idénticos, sólo basta con realizar backups de uno de ellos); el servidor que contiene los roles de AD y ALS; el servidor que contiene los roles de RDWA, RDCB, RDL.

Para la realización de los respaldos se utilizará la solución que provee Proxmox en forma nativa. Esta herramienta nos permite realizar copias completas de los discos de las VMs y almacenarlas en repositorios remotos, como así también calendarizar su realización de forma automática. En la sección Anexos se muestran los pasos para la programación de un backup en Proxmox.

En nuestro caso, la UTN disponía previamente de un repositorio destinado a el almacenamiento de backups. Se trata de un servidor Windows Server 2012, con el rol Servicios para NFS<sup>41</sup> activado, el cual está físicamente separado de la sala de servidores, de modo de no verse afectado ante una catástrofe en dicho lugar. Para el volcado de los backups en dicho repositorio, previamente debe realizarse la conexión al mismo en el clúster de Proxmox. En la sección Anexos se mostrarán los sencillos pasos para la conexión del

---

<sup>39</sup> TCP, por sus siglas en inglés: Transmission Control Protocol.

<sup>40</sup> UDP, por sus siglas en inglés: User Datagram Protocol.

<sup>41</sup> NFS, por sus siglas en inglés: Network File System.

repositorio al clúster de Proxmox como así también la configuración del servidor de almacenamiento mediante el rol de NFS en Windows Server.

## 4.6. Primer etapa de pruebas de rendimiento

Con el objeto de asegurar que las configuraciones llevadas a cabo hasta el momento sean correctas realizamos una prueba de rendimiento que consistió en la ejecución simultánea de aplicaciones virtualizadas sobre 15 equipos de escritorio conectados a la red ethernet cableada de la facultad. Para las pruebas se asignó a cada RDSH: 3 cores de procesador y 16 gb de ram.

Durante la prueba se monitorearon los siguiente indicadores:

- Tráfico en la interfaz de 100 Mbits uplink del switch de acceso de las pcs de escritorio.
- Hardware en los servidores RDSH:
  - Tráfico de red.
  - Uso de memoria ram.
  - Uso de procesador.

### 4.6.1. Pruebas con aplicación Simio 6

La primer prueba se realizó sobre la aplicación Simio 6, ejecutando una simulación durante 2:30 hs. La elección de esta aplicación para la realización de las pruebas se fundamenta en que es uno de los software de la colección más demandantes de recursos de hardware.

En la siguiente tabla se muestran los valores máximos de las mediciones:

Tráfico máximo de Red						Uso máximo de Procesador		Uso máximo de Memoria	
Switch		RDSH1		RDSH2		RDSH1	RDSH2	RDSH1	RDSH2
IN	OUT	IN	OUT	IN	OUT				
2.09 mbps	17.85 mbps	42.67 kbps	233.28 kbps	51.60 kbps	288.86 kbps	100/85.1/78.1	99.5/93/93	7.04 GB	7.21 GB

Tabla 4: 1ra prueba de rendimiento.

#### 4.6.2. Pruebas con aplicación Autocad 2018

La segunda prueba se realizó sobre la aplicación Autocad 2018, durante 1:20 hs. En la siguiente tabla se muestran los valores máximos de las mediciones:

Tráfico máximo de Red						Uso máximo de Procesador		Uso máximo de Memoria	
Switch		RDSH1		RDSH2		RDSH1	RDSH2	RDSH1	RDSH2
IN	OUT	IN	OUT	IN	OUT				
1.44 mbps	1.89 mbps	62.97 kbps	95.32 kbps	62.97 kbps	95.32 kbps	39/83.6/6.1	27.6/46.7/13.5	5.15 GB	4.64 GB

Tabla 5: 2da prueba de rendimiento.

#### 4.6.3. Conclusiones de las pruebas

Al observar la información de las tablas 4 y 5, se observa que los recursos de red no ven comprometidos en ninguna de las pruebas, al verificar que los valores arrojados por las mediciones de tráfico son despreciables en relación al ancho de banda disponible en los equipos.

Con respecto al uso del procesador, durante la prueba realizada con el software Simio puede observarse que la simulación demandó una gran carga de procesamiento, esto no debe interpretarse como una limitación en los recursos, dado que es inherente al tipo de aplicación. Si asignamos más recursos de procesamiento, igualmente se alcanzaría un alto porcentaje de utilización del mismo, viendo la ventaja en la disminución de la duración total de la simulación.

Si observamos todos los indicadores de un RDSH en comparación a los del otro durante una misma prueba, podemos observar la similitud de los mismos debido al balanceo de carga que se hace sobre la ejecución de las aplicaciones.

Finalmente, con los resultados de las pruebas realizadas podemos hacer una primera medición de los recursos de hardware necesarios para el funcionamiento del servicio con 15 clientes y contrastarlos con los recursos asignados previamente, lo que nos permite asegurar

que es posible aumentar la cantidad de clientes soportados o disminuir los recursos asignados en sintonía con los demandados durante el escenario de pruebas.

En la sección Anexos se presentan gráficas de los indicadores monitoreados en cada uno de los recursos de hardware durante las pruebas. Las gráficas son útiles para ver la tendencia de los indicadores en el tiempo, como por ejemplo, en qué momento se alcanzan los valores máximos de uso de procesador, memoria y tráfico de red.

## 5. Etapa 3: Infraestructura de red

### 5.1. Diseño e implementación de topología de red de servidores de procesamiento remoto

En la sección 3.5 presentamos la topología lógica y direccionamiento de red del clúster de servidores. Esta sección está abocada al diseño de la red de los servidores RDSH, dado que estos servidores son los que serán directamente accesibles por los usuarios de las aplicaciones virtualizadas. Es preciso la utilización de una subred específica, distinta a la del resto de los servidores en la infraestructura, para poder hacer un diseño de seguridad exclusivo para dicha red.

En la tabla siguiente se muestra el diseño de red elegido:

Servidor	Dirección IP	Dirección de red	Máscara	Puerta de enlace
RDSH1	10.6.6.1	10.6.0.0	255.255.0.0	10.6.1.1
RDSH2	10.6.6.2	10.6.0.0	255.255.0.0	10.6.1.1

Tabla 6: Direccionamiento IP de RDSH.

Para la utilización de esta red es necesario la creación de una VLAN, nombrada VLAN 6, de modo de poder utilizar las interfaces de red de los servidores físicos del clúster que se conectan al Switch 1 (véase Figura 5) permitiendo tráfico de la red 10.1.4.0/24 de administración (véase Tabla 3) y de la red 10.6.0.0/16 de los RDSH sobre las mismas interfaces de los enlaces entre los nodos y el switch.

En la sección Anexos correspondiente a la sección 3.5 se muestran los parámetros de configuración de la red de servidores de procesamiento remoto, tanto en los servidores del clúster como en el switch de intranet.

## **5.2. Diseño e implementación de topología de red de clientes (servidor DHCP)**

### **5.2.1. Diseño lógico de la red de clientes**

Es preciso identificar a los usuarios de las aplicaciones virtualizadas, para lo cual se diseñó una red específica que nos permita realizar las configuraciones necesarias para la finalidad de la aplicación. En la tabla siguiente se presentan los parámetros de la red de clientes:

Dirección de red	Máscara	Puerta de enlace	Rango de direcciones
10.1.165.0	255.255.255.0	10.1.165.1	10.1.165.150-10.1.165.200

Tabla 7: Direccionamiento IP de clientes.

También se creó una Vlan asociada a la red de clientes (vlan 165) para poder configurar los dispositivos de red involucrados en la topología (switches de distribución, de acceso y access point).

La asignación de las direcciones IP a los clientes se hace mediante DHCP<sup>42</sup> por medio de un servidor de uso general en la facultad.

### **5.2.2. Diseño físico de la red clientes**

La topología de red se basa en una arquitectura jerárquica de tres capas independientes: Núcleo, Distribución, Acceso. Cada capa del diseño desempeña una función específica. La división de la red en capas mantiene los problemas de la red aislados por capas, simplifica el diseño, la implementación y la administración y ayuda a seleccionar el equipo y las características que va a necesitar la red.

---

<sup>42</sup> DHCP, por sus siglas en inglés: Dynamic Host Configuration Protocol. es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.



La capa de acceso es el punto en el que cada usuario, cada terminal, cada grupo de trabajo se conecta a la red.

La capa de distribución es el límite entre las capas de acceso y la capa de núcleo y su conectividad se basa en políticas.

La capa de núcleo proporciona una conmutación de paquetes de alta velocidad.

Dependiendo de las dimensiones de la red, puede emplearse un diseño de red de núcleo contraído o diseño jerárquico de dos niveles. En este modelo de red la capa de distribución y la capa de núcleo se combinan en una sola capa y las funciones de ambas capas se implementan en un solo dispositivo de red. La implementación de un modelo de núcleo contraído supone una reducción de los costos de red sin perder las ventajas del modelo jerárquico de tres niveles.

Cabe aclarar que para nuestra aplicación práctica usamos la topología física ya existente en la UTN FRSF, sólo incorporando los APs y realizando las configuraciones necesarias para incorporar la red de clientes de aplicaciones remotas.

En la figura siguiente se presenta parcialmente la topología física de la red de clientes.

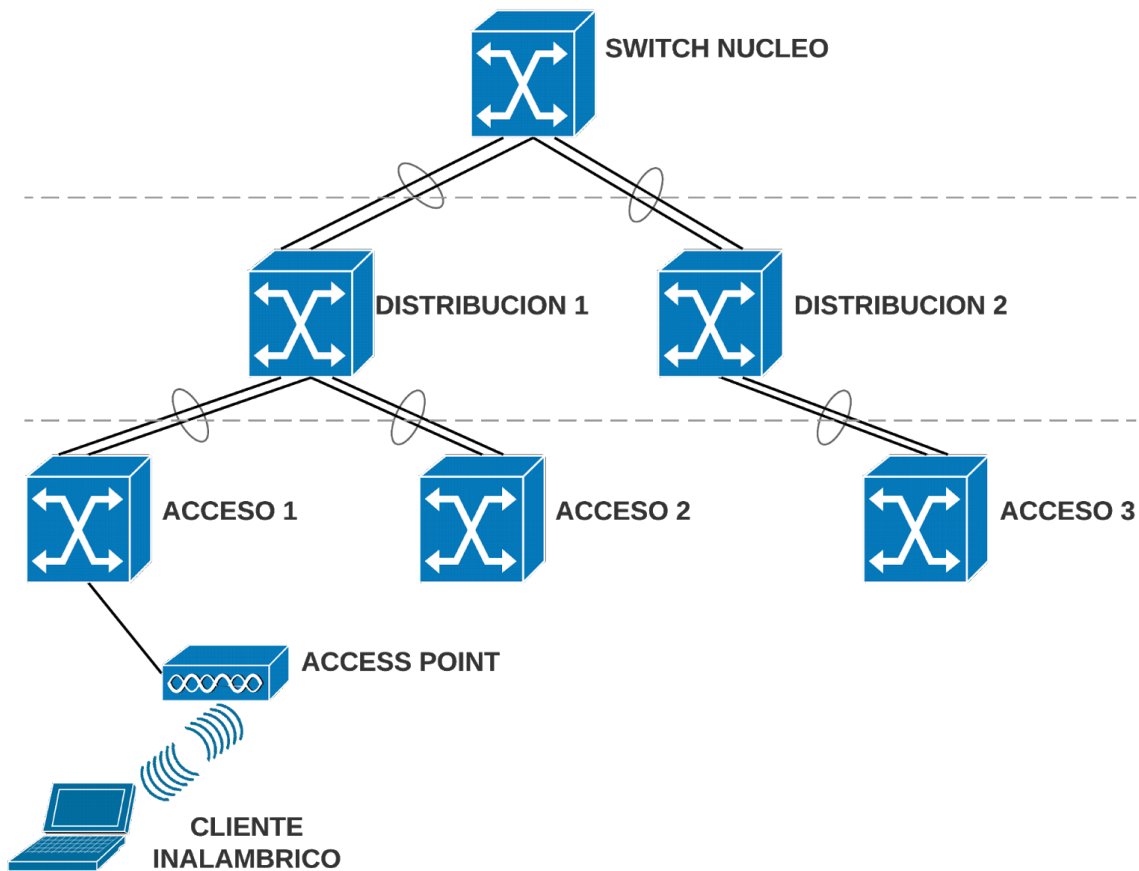


Figura 10: Topología física de red de clientes.

### 5.3. Diseño y configuración de puntos de acceso inalámbrico a la red de clientes

El acceso físico a la red configurada en el apartado anterior se hará por medio de una red wifi. Como mencionamos anteriormente, los clientes de las aplicaciones virtualizadas utilizarán notebooks para acceder al servicio, por lo que el acceso por medios inalámbricos es el más adecuado. Sumado a esto, la característica de la portabilidad asociada a las redes wifi, hace que este medio sea el más adecuado en relación al requerimiento de permitir un despliegue del servicio en diferentes lugares (aulas de la facultad, salas, etc.) en forma fácil y rápida.

Se considera a las redes wifi como extensiones de las redes cableadas, siendo la principal diferencia con éstas la configuración de los dispositivos físicos en sí (access point, controlador).

En general, los AP (access point) se pueden catalogar como AP autónomos o AP basados en controlador:

- AP autónomos: son dispositivos autónomos que se configuran individualmente y son útiles cuando solo se requieren un par de AP en la red. En los AP autónomos toda la configuración reside en el dispositivo. Si aumentaran las demandas inalámbricas y se requerirían más AP, cada AP funcionaría de manera independiente de los otros AP y requeriría una configuración y una administración manuales.
- AP basados en controlador: son dispositivos que dependen del servidor y no requieren una configuración inicial. Los AP basados en controladores son útiles en situaciones en las que se requieren muchos AP en la red. A medida que se agregan más AP, un controlador de WLAN configura y administra cada AP automáticamente.

En la UTN FRSF se dispone de una solución de conectividad wifi basada en controlador de la marca Ubiquiti. Si bien la configuración cuenta con un controlador, este sólo se utiliza para el despliegue de configuraciones en los AP y para obtener información en tiempo real, de modo que la configuración de los AP reside en los mismos y no en el controlador. Esto permite que los AP puedan funcionar independientemente de que el controlador esté en funcionamiento.

Para poder desplegar una red wifi con las características descritas en el apartado 5.2, sólo se debe configurar un SSID descriptivo (en nuestro caso LABMOVIL) y password, y la vlan en la cual va a prestar servicio (VLAN 165). De este modo, los clientes que se conecten a la WLAN LABMOVIL recibirán un dirección ip dinámica por medio del servidor DHCP en la red 10.1.165.0/24. En lo que respecta a los switches de la Figura 10, en los switches de Acceso se deben configurar los puertos en los que se van a conectar los AP de modo que permitan el tráfico de la Vlan 165 y del mismo modo extender las configuraciones a los switch de Distribución. En apartado Anexos se presentan las configuraciones básicas del controlador y de los switches de la topología.

## 5.4. Análisis, diseño e implementación de seguridad en las redes (Access Control List)

Por tratarse la red de clientes de una red de acceso público, es necesario definir con claridad el alcance de la red, de modo de saber con certeza a qué puede y a qué no puede accederse desde dicha red. Es evidente que la red de clientes debe tener acceso a la red de servidores (véase apartado 5.1) de modo de permitir la utilización del servicio de virtualización de aplicaciones, pero además permitiremos el acceso a internet ya que sería poco práctico tener que cambiar de red wifi para acceder a internet al mismo tiempo que se utilizan las aplicaciones virtualizadas.

Para la aplicación de los controles de acceso de la red, haremos uso de las Listas de Control de Acceso (ACL<sup>43</sup>) configuradas directamente sobre los switch de Distribución de la Figura 10.

Los administradores utilizan las ACL para detener el tráfico o para permitir solamente tráfico específico en sus redes.

Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar) conocidas como “entradas de control de acceso” (ACE<sup>44</sup>). Las ACE también se denominan comúnmente “instrucciones de ACL”. Las ACE se pueden crear para filtrar tráfico según ciertos criterios, como la dirección de origen, la dirección de destino, el protocolo y los números de puerto. Cuando el tráfico de la red atraviesa una interfaz configurada con una ACL, el enrutador compara la información dentro del paquete con cada ACE, en orden secuencial, para determinar si el paquete coincide con una de las instrucciones. Si se encuentra una coincidencia, el paquete se procesa según corresponda. De esta manera, se pueden configurar ACL para controlar el acceso hacia o desde una red o a una subred. Se pueden configurar ACL para todos los protocolos de red enrutada.

Para evaluar el tráfico de la red, la ACL extrae la siguiente información del encabezado de capa 3 del paquete:

---

<sup>43</sup> ACL, por sus siglas en inglés: Access Control List.

<sup>44</sup> ACE, por sus siglas en inglés: Access Control Entries.

- Dirección IP de origen
- Dirección IP de destino
- Tipo de mensaje ICMP<sup>45</sup>

La ACL también puede extraer información de capa superior del encabezado de capa 4, incluido lo siguiente:

- Puerto de origen TCP/UDP
- Puerto de destino TCP/UDP

Cuando se las configura, las ACL realizan las siguientes tareas:

- Limitan el tráfico de la red para aumentar su rendimiento. Por ejemplo, si la política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que bloqueen el tráfico de video. Esto reduciría considerablemente la carga de la red y aumentaría su rendimiento.
- Proporcionan un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro host acceda a la misma área. Por ejemplo, se puede restringir el acceso a la red de Recursos Humanos a los usuarios autorizados.
- Filtran el tráfico según el tipo de tráfico. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet.
- Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos, como FTP o HTTP.

Las ACL se configuran para aplicarse al tráfico entrante o al tráfico saliente:

- ACL de entrada: los paquetes entrantes se procesan antes de enrutarse a la interfaz de salida. Las ACL de entrada son eficaces, porque ahorran la sobrecarga de enrutar búsquedas si el paquete se descarta. Si las pruebas permiten el paquete, este se procesa para el routing. Las ACL de entrada son ideales para filtrar los paquetes cuando la red

---

<sup>45</sup> ICMP, por sus siglas en inglés: Internet Control Message Protocol.

conectada a una interfaz de entrada es el único origen de los paquetes que se deben examinar.

- ACL de salida: los paquetes entrantes se enrutan a la interfaz de salida y después se procesan mediante la ACL de salida. Las ACL de salida son ideales cuando se aplica el mismo filtro a los paquetes que provienen de varias interfaces de entrada antes de salir por la misma interfaz de salida.

Pueden clasificarse a las ACL en dos tipos:

- ACL estándar: se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan.
- Las ACL extendidas filtran paquetes IP según varios atributos:
  - Tipo de protocolo
  - Dirección IPv4 de origen
  - Dirección IPv4 de destino
  - Puertos TCP o UDP de origen
  - Puertos TCP o UDP de destino
  - Información optativa de tipo de protocolo para un control más preciso

Dadas las condiciones de nuestro escenario emplearemos ACL de entrada aplicadas sobre el tráfico entrante a los puertos de los switch de Distribución que se conectan a los switch de Acceso que tienen conectados los AP. Las ACL aplicadas serán de tipo Extendidas, dado que de esta manera podemos hacer un filtrado más preciso del tráfico según su origen, destino y puerto.

A continuación se presenta una definición de ACL aplicable a nuestro escenario:

```
acl number 1165
```

```
rule 10 permit icmp icmp-type echo
```

```
rule 11 permit icmp icmp-type echo-reply
```

```
rule 12 permit udp destination-port eq bootps
```

```
rule 30 permit ip source 10.1.165.0 0.0.0.255 destination 10.6.6.1 0.0.0.0 3389
```

*rule 31 permit ip source 10.1.165.0 0.0.0.255 destination 10.6.6.2 0.0.0.0 3389*

*rule 42 permit ip source 10.1.165.0 0.0.0.255 destination 192.168.254.0 0.0.0.255*

*rule 45 permit ip source 10.1.165.0 0.0.0.255 destination 10.200.0.0 0.0.255.255*

*rule 46 deny ip source 10.1.165.0 0.255.255.255*

En esta ACL se permite el tráfico necesario para la solicitud y obtención de una dirección IP por medio del protocolo DHCP (reglas 10, 11 y 12), se permiten las conexiones RDP hacia los servidores RDSH (reglas 30 y 31), se permite el tráfico y finalmente se deniega cualquier otro tipo de tráfico (regla 46).

En la sección Anexos se muestran los conceptos teóricos y recomendaciones para la creación de una ACL.

## 5.5. Segunda etapa de pruebas de rendimiento

En esta ocasión se realizó una prueba consistente en la ejecución simultánea de aplicaciones virtualizadas sobre 15 notebooks conectados a una red inalámbrica. Para las pruebas se asignaron los mismos recursos de hardware que en las pruebas previas.

Durante la prueba se monitorearon:

- Hardware en los servidores RDSH y Access Point:
  - Tráfico de red.
  - Uso de memoria.
  - Uso de procesador.

### 5.5.1. Pruebas con aplicación Simio 6

La primer prueba se realizó sobre la aplicación Simio 6, ejecutando una simulación durante 1:00 hs. En la siguiente tabla se muestran los valores máximos de las mediciones:

Tráfico máximo de Red						Uso máximo de Procesador			Uso máximo de Memoria		
Access Point		RDSH1		RDSH2		Access Point	RDSH1	RDSH2	Access Point	RDSH1	RDSH2
IN	OUT	IN	OUT	IN	OUT						

731.5 kbps	130.6 kbps	53.9 kbps	203.1 kbps	52.6 kbps	302.1 kbps	4	100/75.7/7 5.7	100/93.9/ 93.8	23 MB	6.52 GB	7.04 GB
---------------	---------------	--------------	---------------	--------------	---------------	---	-------------------	-------------------	-------	------------	------------

Tabla 8: 3ra prueba de rendimiento.

### 5.5.2. Pruebas con aplicación Autocad 2018

La segunda prueba se realizó sobre la aplicación Autocad 2018, durante 1:00 hs. En la siguiente tabla se muestran los valores máximos de las mediciones:

Tráfico máximo de Red						Uso máximo de Procesador			Uso máximo de Memoria		
Access Point		RDSH1		RDSH2		Access Point	RDSH1	RDSH2	Access Point	RDSH 1	RDS H2
IN	OUT	IN	OUT	IN	OUT						
240.1 kbps	16.4 kbps	206.6 kbps	361.1 kbps	210.9 kbps	424.0 kbps	3.9	4.8/4.8/0. 95	3.3/3.8/ 1.4	22.78 MB	4.81 GB	5.32 GB

Tabla 9: 4ta prueba de rendimiento.

### 5.5.3. Conclusiones de las pruebas

Observando los resultados de las pruebas realizadas podemos determinar que ninguno de los indicadores está alcanzando valores elevados, por lo que la asignación de los recursos es adecuada e incluso se puede soportar crecimiento de la demanda sin problemas.

Los indicadores más importantes de esta prueba son los relativos a el Access Point, dado que es el único dispositivo que se incorpora en relación a las pruebas de la sección 4.6. Los valores de los indicadores del Acces Point no son alarmantes, siendo el uso de memoria el más elevado, dado que durante la prueba con el software Simio se midió un uso de memoria del 35.82 %. Por experiencias previas con el uso general de los Access Point, el máximo de clientes ronda los 35 simultáneos, por lo que es posible soportar aumentos en la demanda hasta esos límites.

En la sección Anexos se presentan gráficas de los indicadores monitoreados en cada uno de los recursos de hardware durante las pruebas.



## **6. Extensibilidad**

A los fines prácticos de la aplicación del presente proyecto, el alcance del mismo se centró en las instalaciones de la UTN-FRSF. En particular, centramos la aplicación práctica en las necesidades de las cátedras de la carrera de Ingeniería en Sistemas de Información, pero es posible extender el alcance al resto de las cátedras mediante la misma arquitectura propuesta, siendo el equipo tecnológico necesario para ello (servidores, equipos de comunicaciones, etc.) el factor a tener en consideración.

En lo que respecta a lo funcional, nuestro alcance se limitó a aplicaciones de escritorio de uso académico y a usuarios de red WLAN, pero es posible extender su uso a cualquier tipo de aplicación de escritorio y a usuarios de red LAN, como lo pueden ser usuarios de oficina que hacen uso de software de ofimática o software empresariales de uso específico.

Si bien no hicimos hincapié en ello, una característica de la arquitectura propuesta es que permite el rápido despliegue de aplicaciones de escritorio a los usuarios finales en forma centralizada. Esto puede ser particularmente útil en situaciones en las que se requiera la utilización de un software de escritorio por parte de un grupo de usuarios en forma esporádica. Por ejemplo, una oficina de área contable podría requerir la utilización de un software fiscal en una determinada época del año y que en cada período requiera la instalación de una nueva versión o parche.

Finalmente, vale la pena aclarar que la arquitectura diseñada es totalmente escalable, siendo que es posible ampliar su alcance y poder de procesamiento incorporando más recursos tecnológicos como servidores y equipos de comunicaciones. Esto permitiría, por ejemplo, desplegar el servicio en las aulas de consulta de la facultad, de modo que los estudiantes puedan acceder a las aplicaciones fuera de los horarios de laboratorio con sus computadoras personales.

## **7. Conclusiones**

A lo largo de las diferentes etapas de este informe hemos visto los elementos necesarios para la implementación completa de una infraestructura que permite dar solución a distintas

necesidades tecnológicas, que van desde el acceso a un software académico hasta la administración de un parque informático.

Si bien nuestra problemática inicial era la de permitir el acceso a las aplicaciones de software con equipos personales, a lo largo del proyecto fuimos descubriendo diversas ventajas relacionadas con la solución propuesta. Algunas de las ventajas de la solución propuesta son:

- Basada en los recursos disponibles: un punto destacable de la solución desarrollada es que se realizó partiendo de la base de los recursos tecnológicos disponibles y sin la necesidad de incorporar hardware o software nuevo que represente un costo para la implementación.
- Posterga la obsolescencia tecnológica: el principio del procesamiento centralizado hace posible el acceso a aplicaciones de escritorio desde equipos informáticos que no posean los requerimientos mínimos de hardware necesarios para su ejecución.
- Administración centralizada: la centralización de las aplicaciones en servidores de procesamiento permite una administración más simple por parte del personal informático. Tareas como el despliegue de nuevas aplicaciones, actualizaciones, configuraciones, aplicación de licencias o instalación de parches pueden hacerse en forma centralizada sin necesidad de operar sobre las computadoras clientes.
- Posibilidad de escalar la solución, de manera que permita acceso a cualquier alumno de la facultad a software licenciado.

## **8. Referencias bibliográficas**

[1] VMWare: Soluciones de tecnología. <https://www.vmware.com/ar/solutions.html>

[2] Turban, E; King, D; Lee, J; Viehland, D (2008). «Chapter 19: Building E-Commerce Applications and Infrastructure». *Electronic Commerce A Managerial Perspective* (5th edición). Prentice-Hall. p. 27.

[3] Wikipedia: Virtualización.

<https://es.wikipedia.org/wiki/Virtualizaci%C3%B3n>

[4] Microsoft Corp. (2007 (updated 2011)). [Infrastructure Planning and Design. Selecting the Right Virtualization Technology](#). Copyright © 2011 Microsoft Corporation. This documentation is licensed to you under the Creative Commons Attribution License.

[5] VMWare: virtualización. <https://www.vmware.com/ar/solutions/virtualization.html>

[6] Campus Party Ecuador 2015: Consolidación de servidores.

<https://campuse.ro/events/campus-party-ecuador-2015/talk/consolidacion-de-servidores-s-antiago-jara/>

[7]VMWare Docs: Aspectos básicos de la virtualización de CPU.

<https://docs.vmware.com/es/VMware-vSphere/6.5/com.vmware.vsphere.resmgmt.doc/GUID-DFFA3A31-9EDD-4FD6-B65C-86E18644373E.html>

[8] Manual de Xenserver 6.2. <http://www.miniacademia.es/manual-citrix-xenserver/>

[9] Evolución de la estrategia IT apoyada por la Virtualización.

<https://studylib.es/doc/8726728/evoluci%C3%B3n-de-la-estrategia-it-apoyada-por-la-virtualizaci...>

[10] Proxmox. <https://www.btactic.com/proxmox/>

[11] Conoce cómo funciona Proxmox y cómo usarlo.

[http://911-ubuntu.weebly.com/proxmox\\_como\\_funciona/conoce-como-funciona-proxmox-y-como-usarlo](http://911-ubuntu.weebly.com/proxmox_como_funciona/conoce-como-funciona-proxmox-y-como-usarlo)

[12] Diseño e implementación de un clúster de cómputo de alto rendimiento.

<https://docplayer.es/7963735-Diseno-e-implementacion-de-un-cluster-de-computo-de-alto-rendimiento.html>

[13] Wikipedia: Alta disponibilidad. [https://es.wikipedia.org/wiki/Alta\\_disponibilidad](https://es.wikipedia.org/wiki/Alta_disponibilidad)

[14] Arquitectura de RDS y sus roles principales.

<https://blogs.technet.microsoft.com/latam/2017/07/20/arquitectura-de-remote-desktop-servicios-rds-y-sus-roles-principales/>

[15] Setup RD Licensing Role on Windows Server 2012 R2.

<https://www.virtuallyboring.com/setup-rd-licensing-role-on-windows-server-2012-r2/>

[16] Windows Server 2012: Remote Desktop – Quick Start.

<https://windowserver.wordpress.com/2012/10/05/windows-server-2012-remote-desktop-quick-start-parte-1/>

[17] License Administrator Guide. PN: FNP-11110-LAG00. Product Release Date: August 2012.

[18] Wikipedia: Active Directory. [https://es.wikipedia.org/wiki/Active\\_Directory](https://es.wikipedia.org/wiki/Active_Directory)

[19] Wikipedia: Diseño jerárquico de la red.

[https://es.wikipedia.org/wiki/Dise%C3%B1o\\_jer%C3%A1rquico\\_de\\_la\\_red](https://es.wikipedia.org/wiki/Dise%C3%B1o_jer%C3%A1rquico_de_la_red)

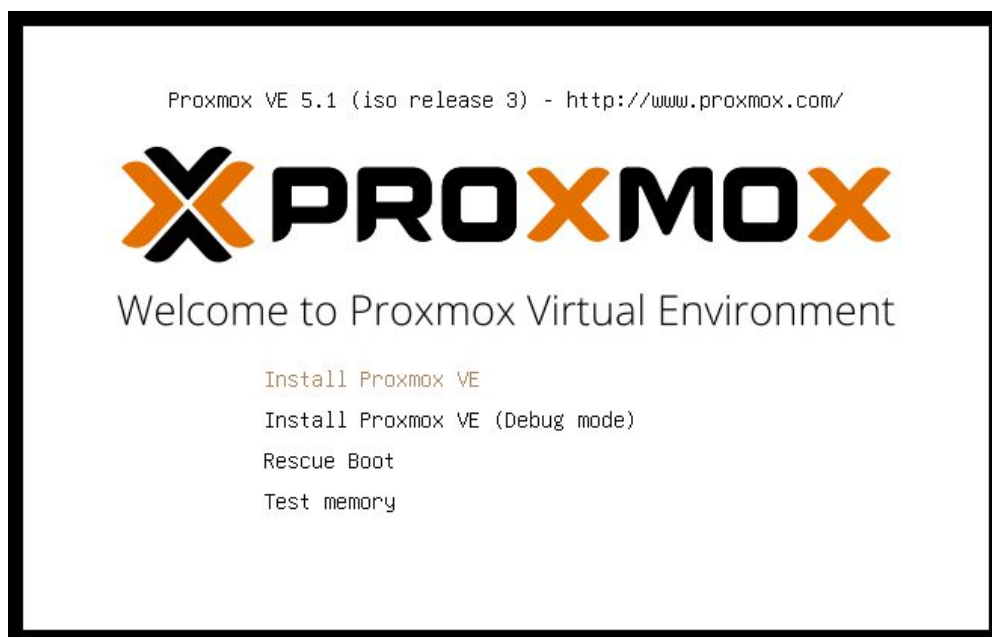
[20] CCNA. <https://www.netacad.com>

## 9. Anexos

### Instalación de PROXMOX VE

Inserte el CD-ROM de instalación, luego arranque desde esa unidad. Inmediatamente después puede elegir las siguientes opciones de menú:

Normalmente, selecciona Instalar Proxmox VE para iniciar la instalación. Después de eso, se le pedirá que seleccione los discos duros de destino. El botón Opciones le permite seleccionar el sistema de archivos de destino, que por defecto es ext4. El instalador usa LVM si selecciona ext3, ext4 o xfs como sistema de archivos, y ofrece una opción adicional para restringir el espacio de LVM.



Normalmente, selecciona Instalar Proxmox VE para iniciar la instalación. Después de eso, se le pedirá que seleccione los discos duros de destino. El botón Opciones le permite seleccionar el sistema de archivos de destino, que por defecto es ext4. El instalador usa LVM si selecciona ext3, ext4 o xfs como sistema de archivos, y ofrece una opción adicional para restringir el espacio de LVM.

También puede utilizar ZFS como un sistema de archivos. ZFS admite varios niveles de software RAID, por lo que es especialmente útil si no tiene un controlador RAID de

hardware. El botón Opciones le permite seleccionar el nivel de RAID de ZFS, y puede elegir los discos allí. También puede configurar opciones adicionales.



La página siguiente solo solicita opciones de configuración básicas como su ubicación, la zona horaria y la distribución del teclado. La ubicación se utiliza para seleccionar un servidor de descarga cerca de usted para acelerar las actualizaciones. Por lo general, el instalador puede detectar esas configuraciones automáticamente, por lo que solo necesita cambiarlas en situaciones excepcionales cuando la detección automática falla, o cuando desea usar una distribución de teclado especial que no se usa comúnmente en su país.

### Location and Time Zone selection

The Proxmox Installer automatically makes location based optimizations, like choosing the nearest mirror to download files. Also make sure to select the right time zone and keyboard layout.

Press the Next button to continue installation.

- **Country:** The selected country is used to choose nearby mirror servers. This will speedup downloads and make updates more reliable.
- **Time Zone:** Automatically adjust daylight saving time.
- **Keyboard Layout:** Choose your keyboard layout.

Country

Time zone

Keyboard Layout

Abort

Next

A continuación, debe especificar una dirección de correo electrónico y la contraseña del superusuario (root). La contraseña debe tener al menos 5 caracteres, pero recomendamos encarecidamente usar contraseñas más seguras.



## Administration Password and E-Mail Address

**Proxmox Virtual Environment** is a full featured highly secure GNU/Linux system based on Debian.

Please provide the *root* password in this step.

- **Password:** Please use a strong password. It should have 8 or more characters. Also combine letters, numbers, and symbols.

- **E-Mail:** Enter a valid email address. Your Proxmox VE server will send important alert notifications to this email account (such as backup failures, high availability events, etc.).

Press the Next button to continue installation.

Password

Confirm

E-Mail

Abort

Next

El último paso es la configuración de la red. Tenga en cuenta que puede utilizar IPv4 o IPv6 aquí, pero no ambos. Si desea configurar un nodo de doble stack, puede hacerlo fácilmente después de la instalación.



### Management Network Configuration

**Please verify** the displayed network configuration. You will need a valid network configuration to access the management interface after installation.

Afterwards press the Next button to continue installation. The installer will then partition your hard disk and start copying packages.

- **IP address:** Set the IP address for the Proxmox Virtual Environment.
- **Netmask:** Set the netmask of your network.
- **Gateway:** IP address of your gateway or firewall.
- **DNS Server:** IP address of your DNS server.

Management interface:	ens3 - 52:54:00:12:34:56 (e1000) ▾
Hostname (FQDN):	node1.yourdomain.tld
IP Address:	192.168.2.179
Netmask:	255.255.240.0
Gateway:	192.168.2.1
DNS Server:	192.168.2.121

Abort

Next

Si presiona Siguiente ahora, la instalación comienza a formatear los discos y copia los paquetes al destino. Espere hasta que termine, luego reinicie el servidor.

La configuración adicional se realiza a través de la interfaz web de Proxmox. Simplemente apunte su navegador a la dirección IP proporcionada durante la instalación ([https:// youripaddress: 8006](https://youripaddress:8006)).



## Proxmox VE Installer

### Virtualize your IT Infrastructure

Proxmox VE is ready for enterprise deployments.

The role based permission management combined with the integration of multiple external authentication sources is the base for a secure and stable environment.

Visit [www.proxmox.com](http://www.proxmox.com) for more information about commercial support subscriptions.

- **Commitment to Free Software**  
The source code is released under the GNU Affero General Public License.
- **RESTful web API**  
Resource Oriented Architecture (ROA) and declarative API definition using JSON Schema enables easy integration for third party management tools.
- **Virtual Appliances**  
Pre-installed applications - up and running within a few seconds.

extracting bash-completion\_2.1-4.3\_all.deb  
50%

Abort

Next

### Creación del Cluster

Para crear el cluster en Proxmox introducimos el siguiente comando:

- Debemos estar en uno de los futuros nodos y crear el cluster, en este caso empezamos por el Nod01:

```
[root@nod01 ~]# pvecm create clusterproxmox
```

- Para chequear que el nodo está anexo al cluster:

```
[root@nod01 ~]# pvecm status
```

```
Quorum information
```

```
-----
```

```
Date: Fri Jan 5 14:26:58 2018
```

```
Quorum provider: corosync_votequorum
```

```
Nodes: 3
```

```
Node ID: 0x00000001
```

Ring ID: 1/3972

Quorate: Yes

Votequorum information

-----

Expected votes: 3

Highest expected: 3

Total votes: 3

Quorum: 2

Flags: Quorate

Membership information

-----

Nodeid	Votes	Name
0x00000001	1	10.1.4.10 (local)
0x00000002	1	10.1.4.20

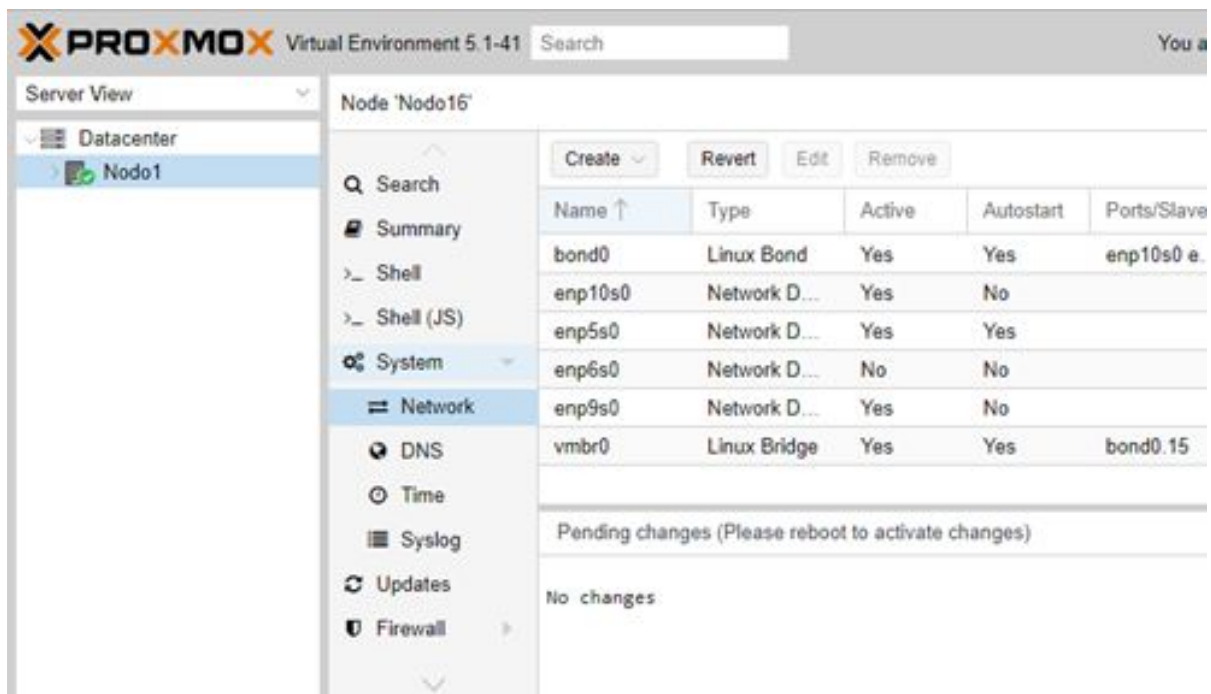
- Para anexar los demás nodos al cluster debemos ingresar por consola a los mismos y colocar el siguiente comando:

```
[root@nodo2 ~]# pvecm add nodo1
```

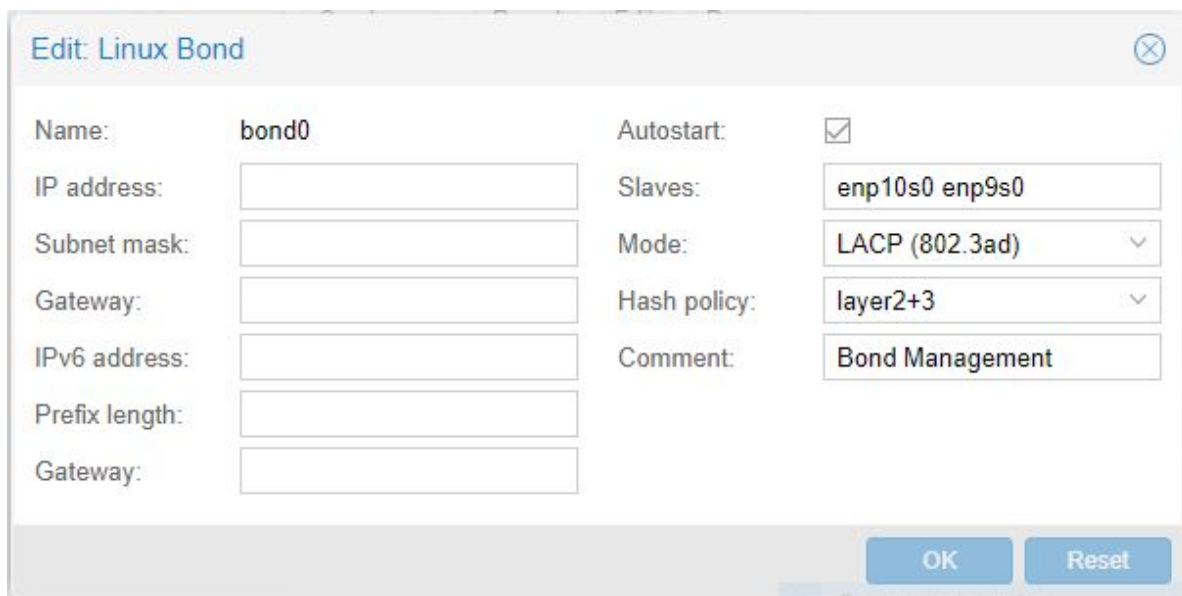
**Nota:** Todo nodo que se quiera anexar se repite la operación. Se puede chequear la información con "pvecm status" o con "pvecm nodes" para solo visualizar la información de los nodos anexados al cluster.

### Creación del Bond

Para crear el bond entre 2 placas de red debemos crear un bond en el menú Network del administrador Web de Proxmox.



Clickeamos en Create y seleccionamos Linux Bond. La configuración queda como se ve en la imagen:



**Nota:** modo bond LACP(802.3ad): Se trata del estandar IEEE 802.3ad (Dynamic link aggregation) también llamado “port trunking“. Permite la definición de agregados ofreciendo alta disponibilidad y un aumento de la velocidad. Para poder configurar este modo necesitamos:

- Soporte de ethtool para obtener la velocidad y el modo del interfaz.
- El switch debe soportar el modo. Por ejemplo los equipos CISCO lo nombran port trunking.

**Slaves:** Colocamos el nombre de las interfaces de red que forman el bond, en este caso enp10s0 y enp9s0.

**Comment:** pequeño comentario de la utilidad del bond. En este caso Bond Management.

**Hash Policy:** layer 2+3.

Una vez reiniciado el nodo los cambios haran efecto.

Continuamos con la creación del Bridge para colocar la ip al bond.

Click en el menú Network/create/bridge linux y dejamos la siguiente configuración:

En el campo **Bridge ports** se referencia el bond creado anteriormente.

### Creación de VLAN Bridge

Para crear el VLAN Bridge debemos hacerlo sobre el bond y especificar la Vlan a la que pertenece dicho Bridge. Se crea haciendo click en el menú Network/create/bridge linux . En el ejemplo se muestran los pasos para la Vlan 6.

Name:	vibr0	Autostart:	<input checked="" type="checkbox"/>
IP address:	<input type="text"/>	VLAN aware:	<input checked="" type="checkbox"/>
Subnet mask:	<input type="text"/>	Bridge ports:	bond 0.6
Gateway:	<input type="text"/>	Comment:	Labmovil
IPv6 address:	<input type="text"/>		
Prefix length:	<input type="text"/>		
Gateway:	<input type="text"/>		

### Activación de forwarding

```
[root@nodo1 ~]# nano /proc/sys/net/ipv4/ip_forward
```

Ponemos valor 1.

**Nota:** esto para cada nodo, en este ejemplo se realizó para el nodo 1.

### Configuración de MTU en interfaces

En las interfaces de red destinadas al tráfico de SAN configuramos tamaño máximo de segmento de 9000.

Vemos que el valor actual de MTU en la interfaz es 1500:

```
root@nodo1:~# ip addr
2: enp6s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UP
group default qlen 1000
    link/ether 18:d6:c7:01:1e:8b brd ff:ff:ff:ff:ff:ff
inet 10.5.10.10/24 brd 10.5.10.255 scope global enp6s0
    valid_lft forever preferred_lft forever
inet6 fe80::1ad6:c7ff:fe01:1e8b/64 scope link
    valid_lft forever preferred_lft forever
```

Editamos el archivo de interfaces del nodo, y agregamos en las interfaces que van al storage la entrada “mtu 9000”.

```
root@nodol1:~# nano /etc/network/interfaces
auto enp6s0
iface enp6s0 inet static
    address 10.5.10.10
    netmask 255.255.255.0
    mtu 9000
#Interfaz 2 Storage
```

Volvemos a verificar el valor en la interfaz:

```
root@nodol1:~# ip addr
2: enp6s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc
pfifo_fast state UP
    group default qlen 1000
    link/ether 18:d6:c7:01:1e:8b brd ff:ff:ff:ff:ff:ff
    inet 10.5.10.10/24 brd 10.5.10.255 scope global enp6s0
    valid_lft forever preferred_lft forever
    inet6 fe80::1ad6:c7ff:fe01:1e8b/64 scope link
    valid_lft forever preferred_lft forever
```

## Conexión de Storage

Configuraciones a realizar en todos los nodos del clúster:

Editar /etc/lvm/lvm.conf y dejar "locking\_type = 3"

```
root@nodol1:~# apt-get install open-iscsi multipath-tools
root@nodol1:~# sed -r -i 's|node.startup = manual|node.startup =
automatic|g' /etc/iscsi/iscsid.conf
```

Cambiamos el nombre del iniciador iSCSI

```
root@nodol1:~# nano /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.1993-08.ar.edu.utn.frsf:nodol1
root@nodol1:~# /etc/init.d/open-iscsi restart
```

```
root@nodol1:~# iscsiadm -m discovery -t sendtargets -p 10.5.10.1
```

```
root@nodol1:~# iscsiadm -m node --login
```

En un nodo cualquiera, además hacer:

```
root@nodol1:~# /lib/udev/scsi_id -g -d /dev/sdb , para obtener el wwid del storage
```

Crear el archivo `/etc/multipath.conf` con el siguiente contenido:

```
defaults {
    user_friendly_names    yes
    polling_interval       2
    path_selector           "round-robin 0"
    path_grouping_policy   multibus
    path_checker           readsector0
    getuid_callout         "/lib/udev/scsi_id -g -u -d
/dev/%n"
    rr_min_io              100
    failback               immediate
    no_path_retry          queue
}
blacklist {
    wwid .*
}
blacklist_exceptions {
    wwid "wwid del storage"
    property "(ID SCSI VPD|ID WWN|ID SERIAL)"
}
multipaths {
    multipath {
        wwid "wwid del storage"
        alias lunPROXMOX
    }
}
```



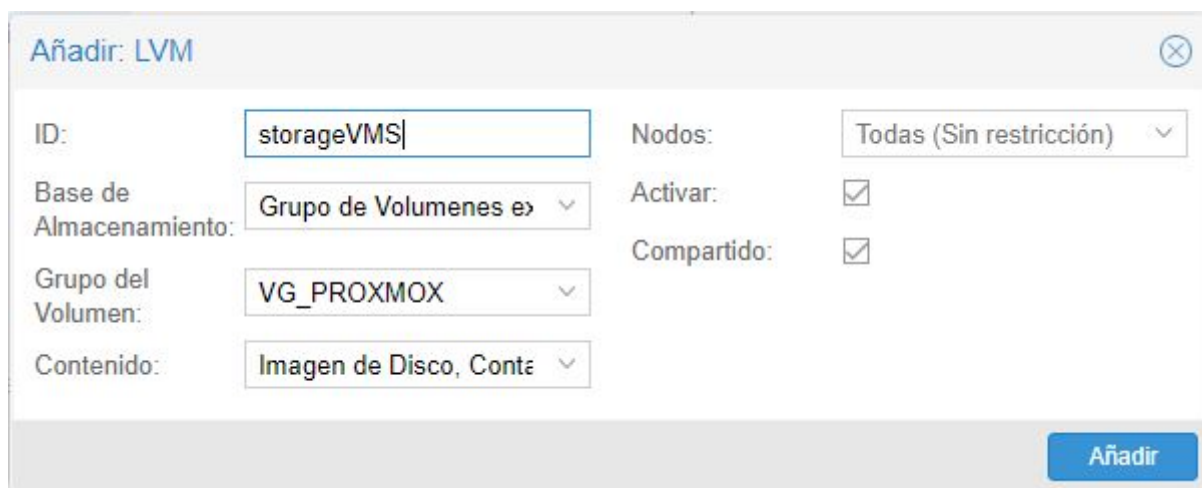
```
}  
root@nodol1:~# modprobe -v dm_multipath  
root@nodol1~# modprobe -v dm_round_robin  
root@nodol1:~# systemctl stop multipath-tools.service  
root@nodol1:~# systemctl start multipath-tools.service
```

Creamos el Physical Volume y el Volume Group:

```
root@nodol1:~# pvcreate /dev/disk/by-id/lunPROXMOX  
root@nodol1:~# vgcreate VG_PROXMOX /dev/mapper/lunPROXMOX
```

Ahora desde la interfaz web:

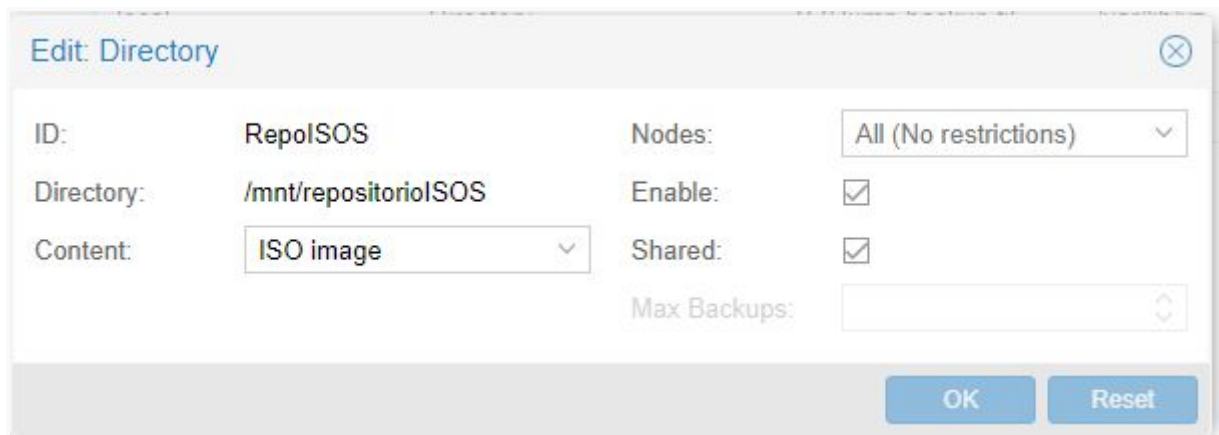
Centro de Datos -> Almacenamiento -> Añadir LVM



ID:	<input type="text" value="storageVMS"/>	Nodos:	<input type="text" value="Todas (Sin restricción)"/>
Base de Almacenamiento:	<input type="text" value="Grupo de Volúmenes ex"/>	Activar:	<input checked="" type="checkbox"/>
Grupo del Volumen:	<input type="text" value="VG_PROXMOX"/>	Compartido:	<input checked="" type="checkbox"/>
Contenido:	<input type="text" value="Imagen de Disco, Contá"/>		

### Montar directorio compartido

Debemos ante todo crear un directorio al que llamaremos RepoISOS (o cualquier otro nombre), esto lo hacemos desde la consola web de administración de PROXMOX por el siguiente camino: Datacenter -> Storage ->add -> Directory



**ID:** Nombre del directorio que aparecerá en el entorno gráfico.

**Directory:** lugar y nombre de la carpeta donde proxmox creará las carpetas necesarias para montar el contenido.

**Content:** qué es lo que va a almacenar la ubicación anterior. En este caso las imágenes ISOS. (Esto es necesario aclarar porque proxmox crea carpetas que guardan distintas cosas, Máquinas virtuales, ISOS, snapshots, etc, y utiliza un método de carpetas para almacenar y dividir el contenido).

**Nodes:** Todos los nodos.

**Enable:** activar.

**Shared:** activar.

Entramos por consola a los nodos para montar la carpeta del repositorio. El username debe corresponder al usuario de log de windows al igual que la contraseña.

```
root@nodol:~# mount -t cifs //10.1.2.12/Instaladores -o
username=adminproxmox /mnt/repositorioISOS/template/iso/
```

Para hacerlo de manera permanente, ya que al reiniciar el nodo se desmonta la unidad:

```
root@nodol:~# nano /etc/fstab
```

Agregamos al final, la siguiente línea:

```
//10.1.2.12/Instaladores /mnt/repositorioISOS/template/iso/
cifs username=adminproxmox,password=<pass> 0 0
```

## Backups y reducción de velocidad

Es posible limitar el uso de ancho de banda de las interfaces de red durante las operaciones de backup para evitar la saturación de las mismas y que afecten al funcionamiento del nodo.

La configuración de este archivo afecta directamente los backups manuales y los que son programados a través de la calendarización.

```
nano /etc/vzdump.conf

# vzdump default settings
#tmpdir: DIR
#dumpdir: /dev/VG_PROXMOX/
dumpdir: /mnt/backupsVMs/
#storage: storageVMS
mode: snapshot
bwlimit: 18000
#ionice: PRI
#lockwait: MINUTES
#stopwait: MINUTES
#size: MB
#stdexcludes: BOOLEAN
#mailto: ADDRESSLIST
maxfiles: 3
#script: FILENAME
#exclude-path: PATHLIST
#pigz: N:
remove: 1
```

**bwlimit:** Límite de ancho de banda para backups. La unidad de medida es el kbit/s. Se realizaron varias pruebas con la infraestructura hardware actual y obtuvimos el menor número de problemas en los IOPS del storage con un ancho de banda de 18000 kbit/s que son equivalentes a 17 MiB/s.

**dumpdir:** Directorio donde se alojan los backups realizados por el calendarizador.

**mode:** Es el tipo de Backup a realizar, el modo snapshot, permite la creación del backup sin necesidad de suspender o apagar la máquina virtual, pero tiene mayor riesgo de incoherencias al permitir la actividad del servidor mientras se realizan las tareas de backup.

**maxfile:** Es el número máximo de backups permitidos por usuario del sistema.

**remove:** Es el número de backups que son removidos cuando se alcanza el límite de backups permitidos. Default es 1.

## HA - comandos e inicio del servicio

El servicio HA se administra a través de GUI en Datacenter->HA

Línea de comandos:

- Adherir servicio HA a una máquina virtual:  
`ha-manager add vm:100`
- Iniciar o parar el servicio:  
`ha-manager set vm:100 --state stopped`  
`ha-manager set vm:100 --state started`
- Ver qué máquinas virtuales tienen el servicio activo y en qué estado se encuentran:  
`ha-manager config`
- Estado del ha manager:  
`ha-manager status`
- Migrar una máquina hacia otro nodo en modo HA:  
`ha-manager migrate vm:100 node2`

Se recomienda crear grupos, uno por cada nodo del clúster y que contenga a todos los nodos. Para cada grupo se debe asignar prioridades decrecientes a cada nodo. Las vms que corran en cada grupo lo harán sobre los nodos de mayor prioridad. Los grupos deben tener habilitada la opción “nofailback” para evitar que al mover intencionalmente una vm de uno nodo a otro, esta vuelva a moverse al nodo de mayor prioridad.

A la hora de crear una VM se la debe asignar a un grupo de forma que la carga se divida equitativamente entre los grupos. Esta configuración se recomienda para evitar que la caída de un nodo provoque movimientos de vms que se encuentran en otros nodos.

## Configuración de Switch de arquitectura de virtualización

### Configuración de Switch de Intranet

El Switch de Intranet del cluster se encarga de comunicar a los nodos con la red de producción. Se conecta directamente a los nodos y al switch de núcleo de la red.

A continuación presentamos la configuración de las interfaces del switch de Intranet:

- Interfaces hacia los nodos: se forman agrupamientos de dos interfaces, en modo troncal y permiten el tráfico de las vlan 1 (administración) y 6 (servidores). La configuración de LACP es en modo dinámico. A continuación se muestra la configuración correspondiente al nodo1:

```
interface Bridge-Aggregation1
  description ProxmoxNodo1
  port link-type trunk
  port trunk permit vlan 1 6
  port trunk pvid vlan 1
  link-aggregation mode dynamic
```

La configuración de los puertos GigabitEthernet1/0/1 y GigabitEthernet1/0/2 es similar.

```
interface GigabitEthernet1/0/1
  description ProxmoxNodo1
  port link-type trunk
  port trunk permit vlan 1 6
  port trunk pvid vlan 1
  broadcast-suppression pps 3000
```

```
stp edged-port enable
port link-aggregation group 1
```

- Interfaces hacia switch de núcleo: se forma un agrupamiento de cuatro interfaces, en modo troncal y permite el tráfico de las vlan 1 y 6.

```
interface Bridge-Aggregation3
description swNucleo
port link-type trunk
port trunk permit vlan 1 6
```

La configuración de los los puertos GigabitEthernet1/0/5 a 8 es similar.

```
interface GigabitEthernet1/0/5
description swNucleo
port link-type trunk
port trunk permit vlan 1 6
broadcast-suppression pps 3000
stp edged-port enable
qos trust dscp
port link-aggregation group 3
```

### **Configuración de Switches de iSCSI**

Los switches de iSCSI forman una red SAN entre los nodos y el Storage.

A continuación presentamos la configuración de las interfaces del switch de iSCSI:

- Interfaces hacia los nodos: se configuran en modo acceso sobre la vlan 7 y con mtu de 9216. Esta vlan es de uso exclusivo de la SAN, por lo que dominio de broadcast sólo comprende este switch. A continuación se muestra la configuración de la interfaz del switch 2 iSCSI hacia el nodo 1:

```
interface ethernet 1/g5
description "ProxmoxNodo1-10.5.20.x"
mtu 9216
```

```
switchport access vlan 7
Exit
```

La configuración del nodo 2 es similar. Las configuraciones en el switch 3 iSCSI es similar empleando la vlan 8.

- Interfaces hacia el storage: se configuran cuatro interfaces en modo acceso sobre la vlan 7 en el switch 2 y vlan 8 en el switch 3. A continuación se muestra la configuración de un puerto del switch 2 de iSCSI:

```
interface ethernet 1/g1
description "StorageA1"
mtu 9216
switchport access vlan 7
Exit
```

La configuración de los puertos 1 a 4 es similar.

### **Configuración de Switch de Núcleo**

El switch de núcleo comunica la red de servidores (10.6.0.0/16) con la red de clientes (10.1.165.0/24). Se encarga de realizar el ruteo entre las redes de las vlan 6 y 165.

A continuación presentamos la configuración de las conexiones hacia el switch de Intranet y hacia los switches de distribución:

- Interfaces hacia switch de Intranet:

```
interface Bridge-Aggregation1
description Intranet
port link-type trunk
port trunk permit vlan 1 6
#
```

La configuración de los los puertos GigabitEthernet1/0/5 a 8 es similar.

```

interface GigabitEthernet1/0/5
  port link-mode bridge
  description Intranet
  port link-type trunk
  port trunk permit vlan 1 6
  broadcast-suppression pps 3000
  undo jumboframe enable
  port link-aggregation group 1
#

```

- Interfaces hacia switches de Distribución: se muestra la conexión hacia uno de los switch por ser similar en ambos.

```

interface Bridge-Aggregation2
  description Distribucion1
  port link-type trunk
  port trunk permit vlan 1 165
#

```

La configuración de los puertos GigabitEthernet1/0/9 y GigabitEthernet1/0/10 es similar.

```

interface GigabitEthernet1/0/9
  port link-mode bridge
  description Distribucion1
  port link-type trunk
  port trunk permit vlan 1 165
  broadcast-suppression pps 3000
  undo jumboframe enable
  qos trust dscp
  port link-aggregation group 2

```

Configuración para realizar el ruteo entre las redes:



```
vlan 6
  description Servidores_LabMovil
#
vlan 165
  description Clientes_LabMovil
interface Vlan-interface6
  ip address 10.6.1.1 255.255.0.0
#
interface Vlan-interface165
  ip address 10.1.165.1 255.255.255.0
#
```

## **Configuración de Storage**

A continuación se muestran las configuraciones realizadas en el Storage (HP P2000 G3 iSCSI) para la creación del espacio de almacenamiento común del clúster de servidores.

En nuestro caso partimos de un vdisk existente configurado con RAID 5, por lo que sólo creamos un Volumen.

**vd02 (RAID5)**


View ▾ Provisioning ▾ Configuration ▾ Tools ▾ Help

vd02 (RAID5) > Provisioning > Create Volume

### Create Volume

Create a volume by assigning a name, selecting a size and setting the default mapping

Volume name\*:


Size:  GB   815

OpenVMS Volume?:  OpenVMS Volume UID:

---

Enable Snapshots:

Standard Policy

Snap Pool:  Reserve Size  6GB  978GB

Attach Pool

Replication Prepare:


---

Map:

LUN\*:  Access:

Select ports from the view or list below:

Graphical  Tabular



Se especifica un nombre, tamaño y un número de LUN para el mapeo de los nodos del clúster.

Finalmente se configuran mapeos explícitos hacia los nodos del clúster.

Volume **Proxmox\_VM** (249.9GB)

View ▾ Provisioning ▾ Configuration ▾ Tools ▾ Help

Volume Proxmox\_VM (249.9GB) > Provisioning > Explicit Mappings

### Explicit Volume Mappings

Modify the volume mappings to specific hosts by using the default map or explicit map settings

Select an item to modify the mapping properties to a specific host:

Maps for Volume Proxmox_VM						
<input type="radio"/>	Explicit	iqn.1993-08.ar.edu.utn.frsf.nodo1	nodo1	A1,A2,A3,A4,B1,B2,B3,B4	10	read-write
<input type="radio"/>	Explicit	iqn.1993-08.ar.edu.utn.frsf.nodo2	nodo2	A1,A2,A3,A4,B1,B2,B3,B4	10	read-write

Map:  (Clear to remove existing mapping)

LUN:\*  Access:

## Implementación de roles de RDS en Windows Server

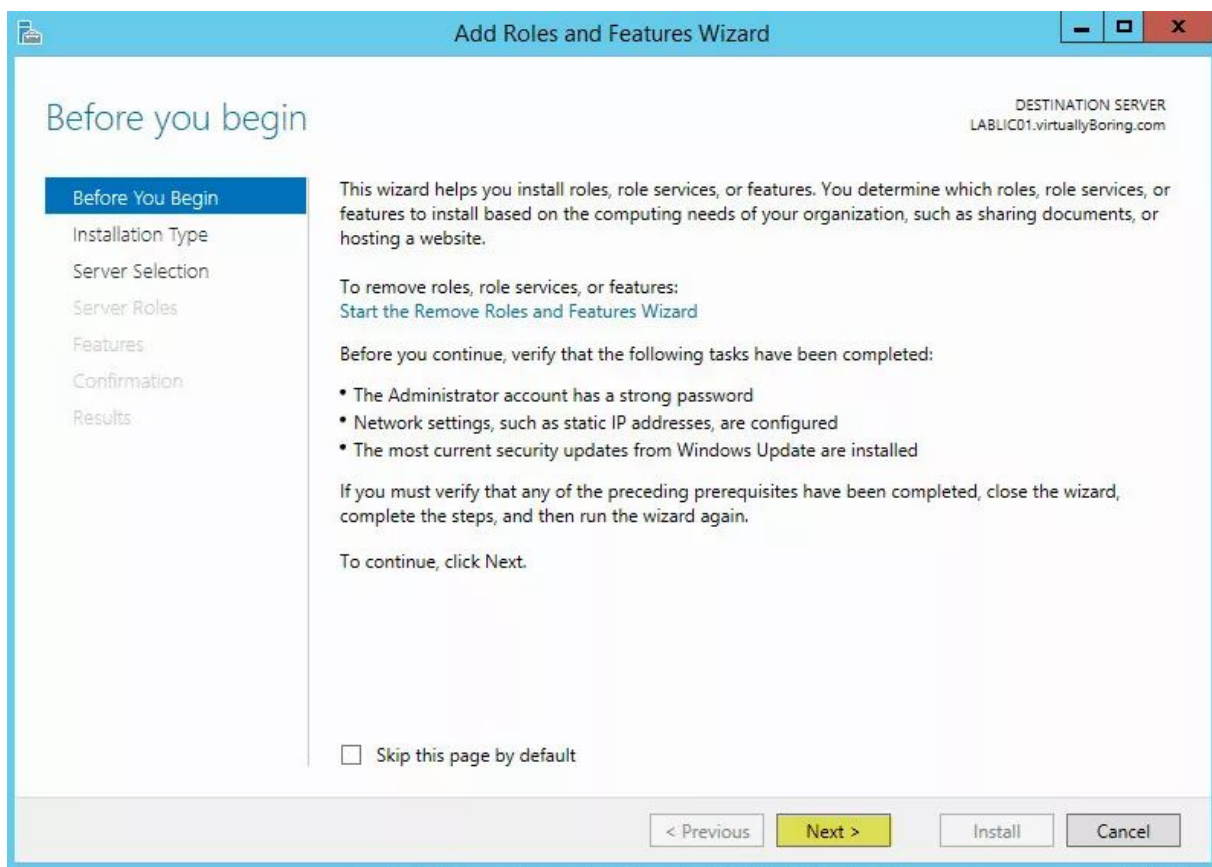
La instalación de los roles necesarios para la arquitectura de RDS se realiza en forma conjunta.

Desde el servidor ir a Manage -> Add Roles and Features.

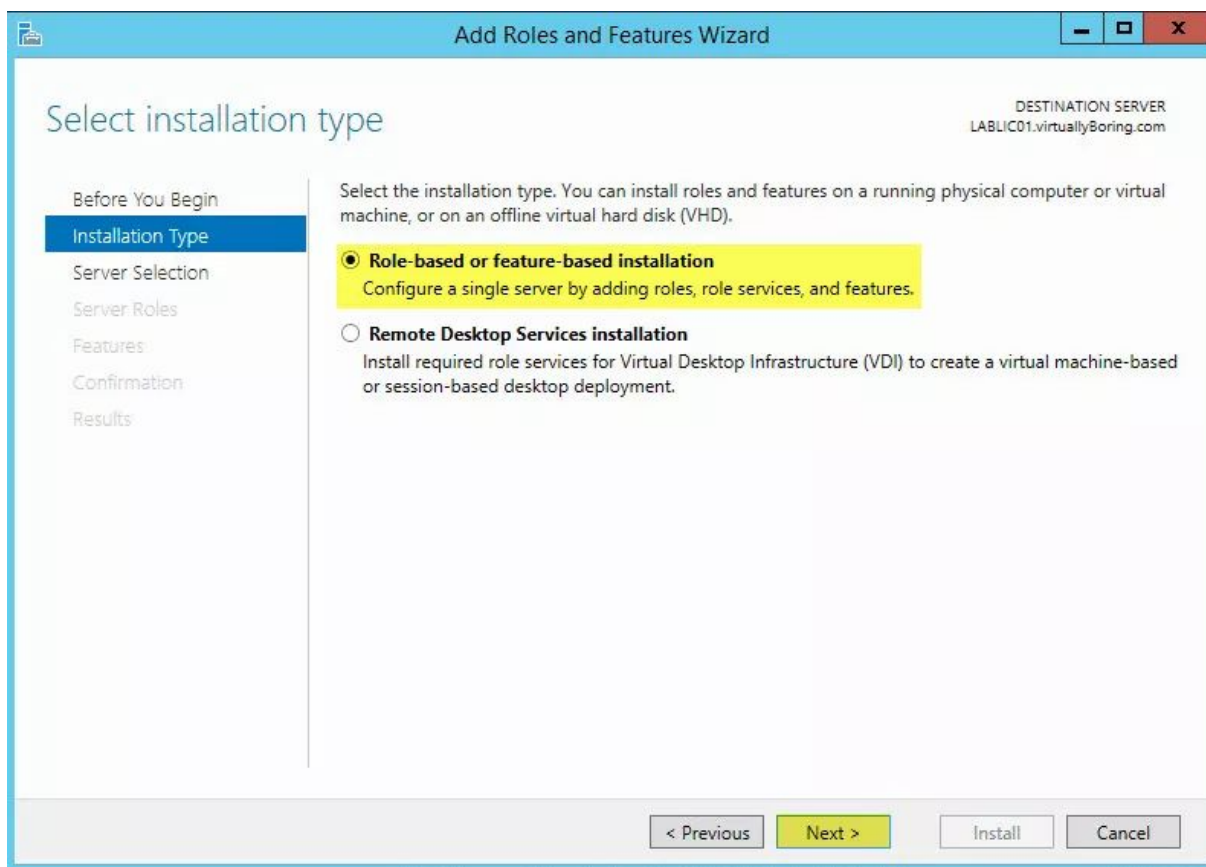
The screenshot shows the Windows Server Manager interface. The 'Manage' menu is open, and 'Add Roles and Features' is highlighted. The main area displays a table of servers:

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
LABLIC01	192.168.1.248	Online	10/31/2015 10:41:03 AM	00252-00106-86557-AA

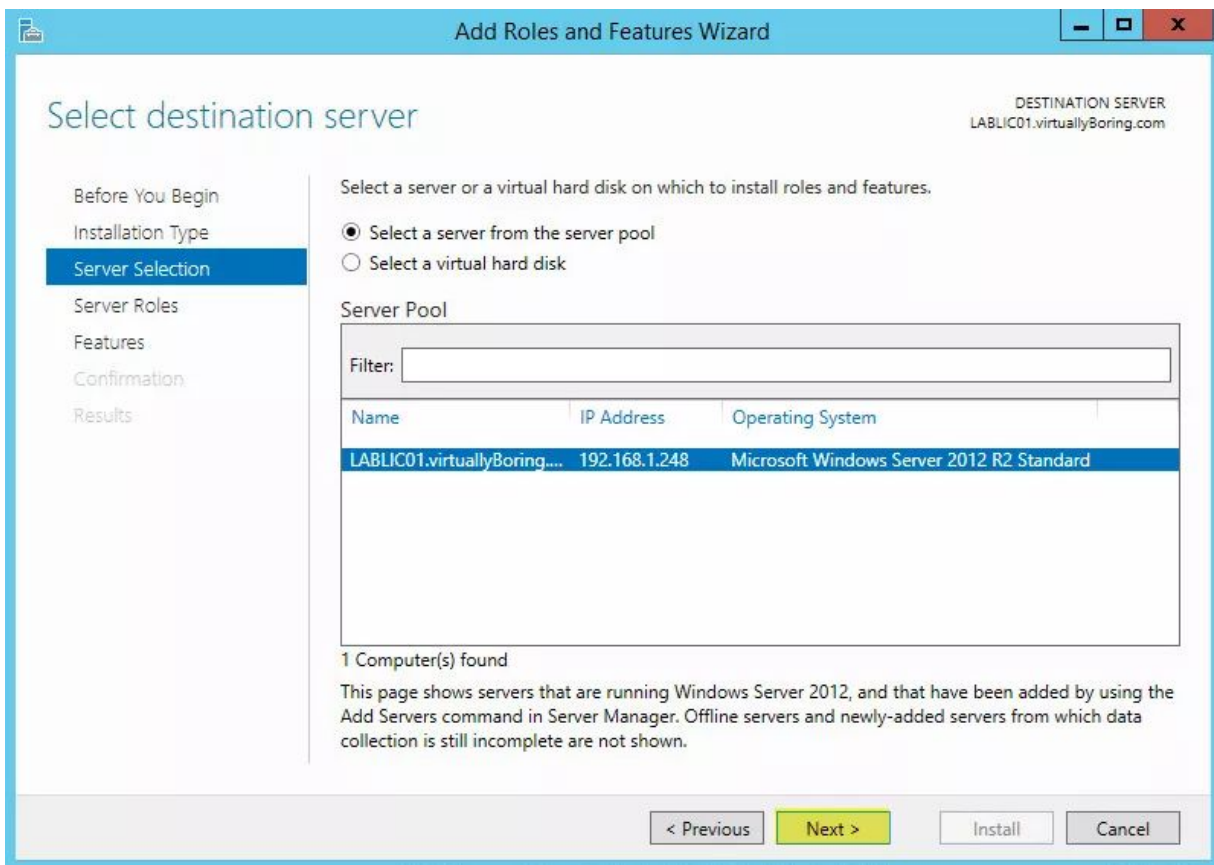
Clickear en Next.



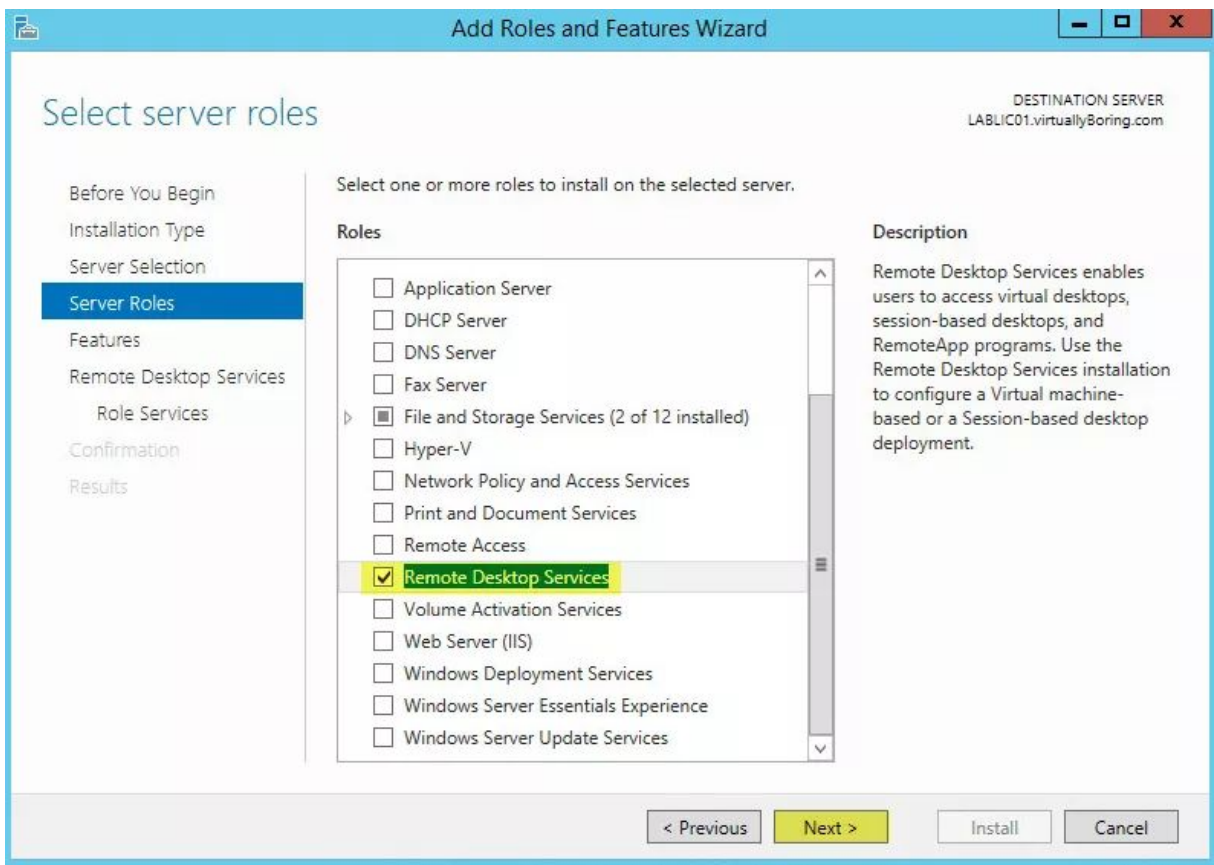
Seleccionar Role-base or feature-based installation y clickear en Next.



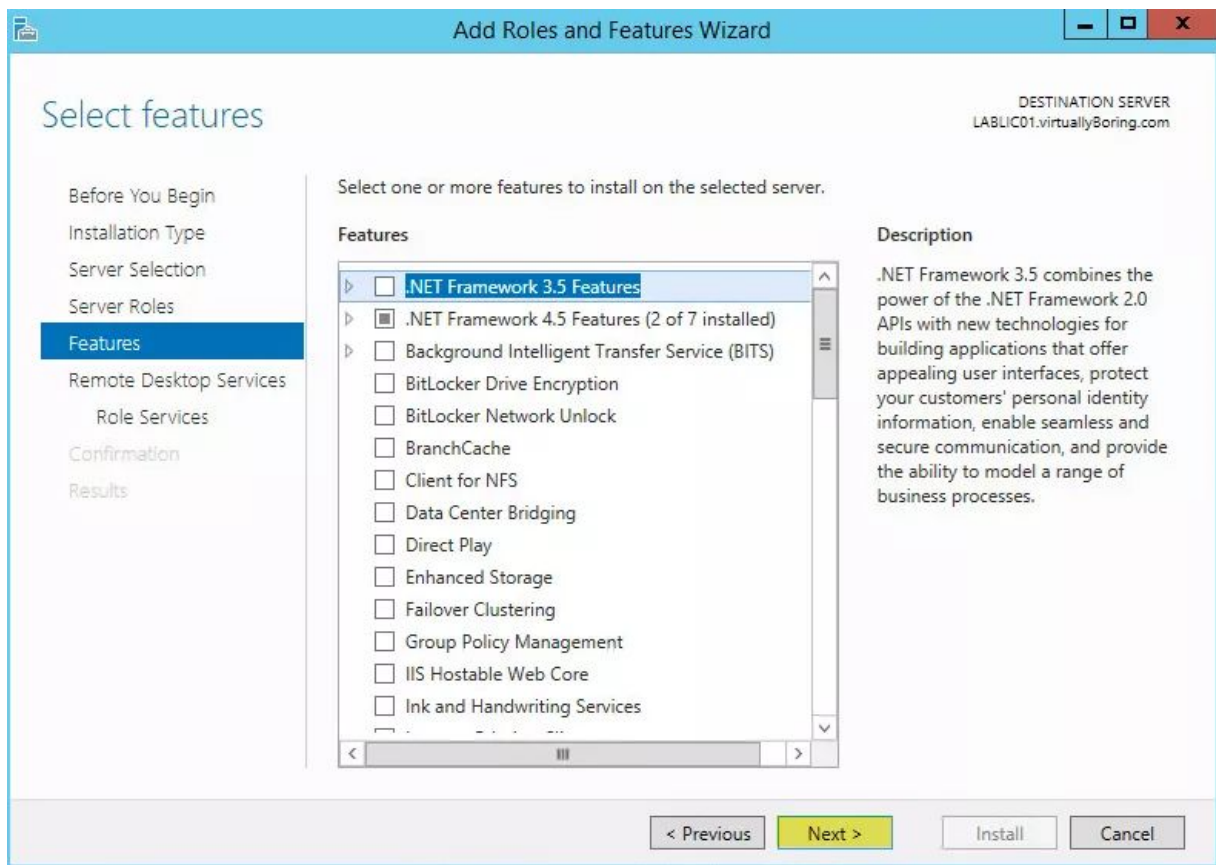
Seleccionar el servidor del pool de servidores. Clickear en Next.



Desplazar hacia abajo y seleccionar Remote Desktop Services, luego clicar en Next.

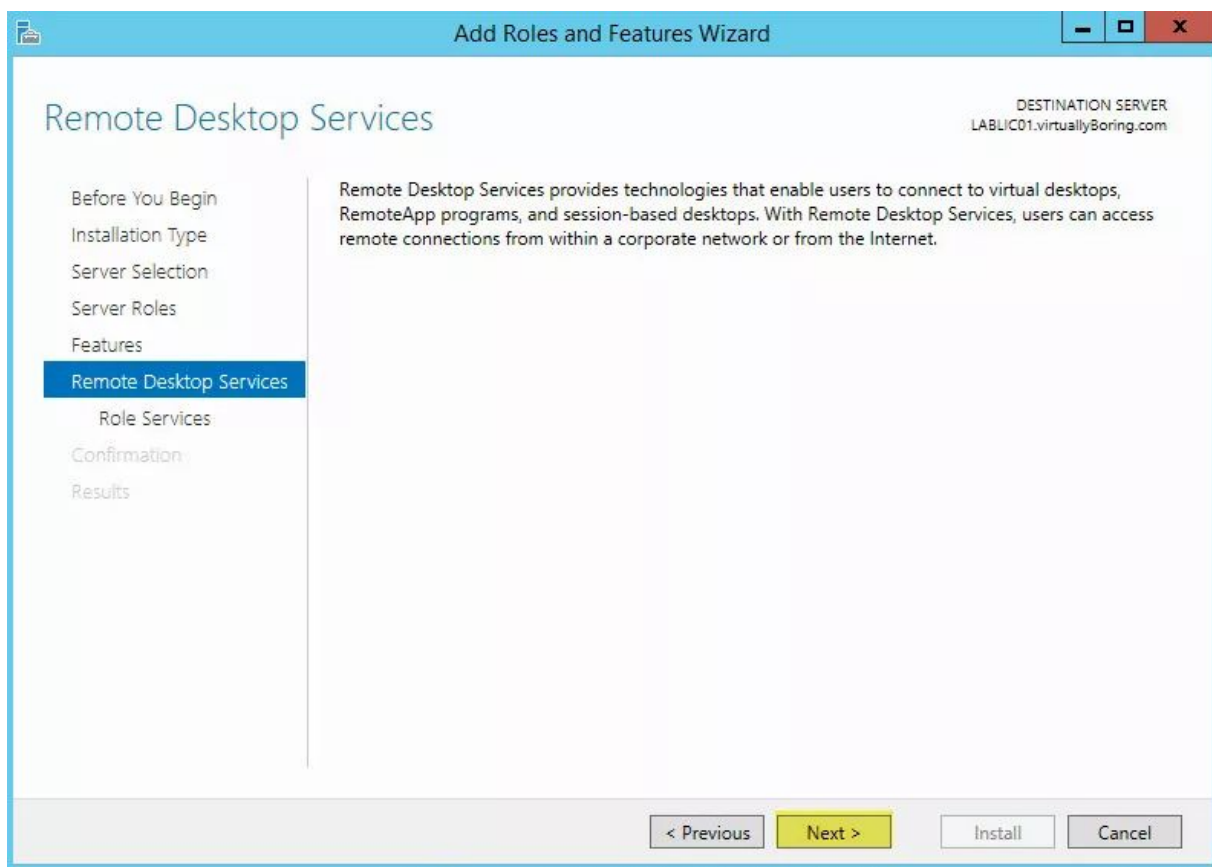


Clickear en Next sin seleccionar una Feature.

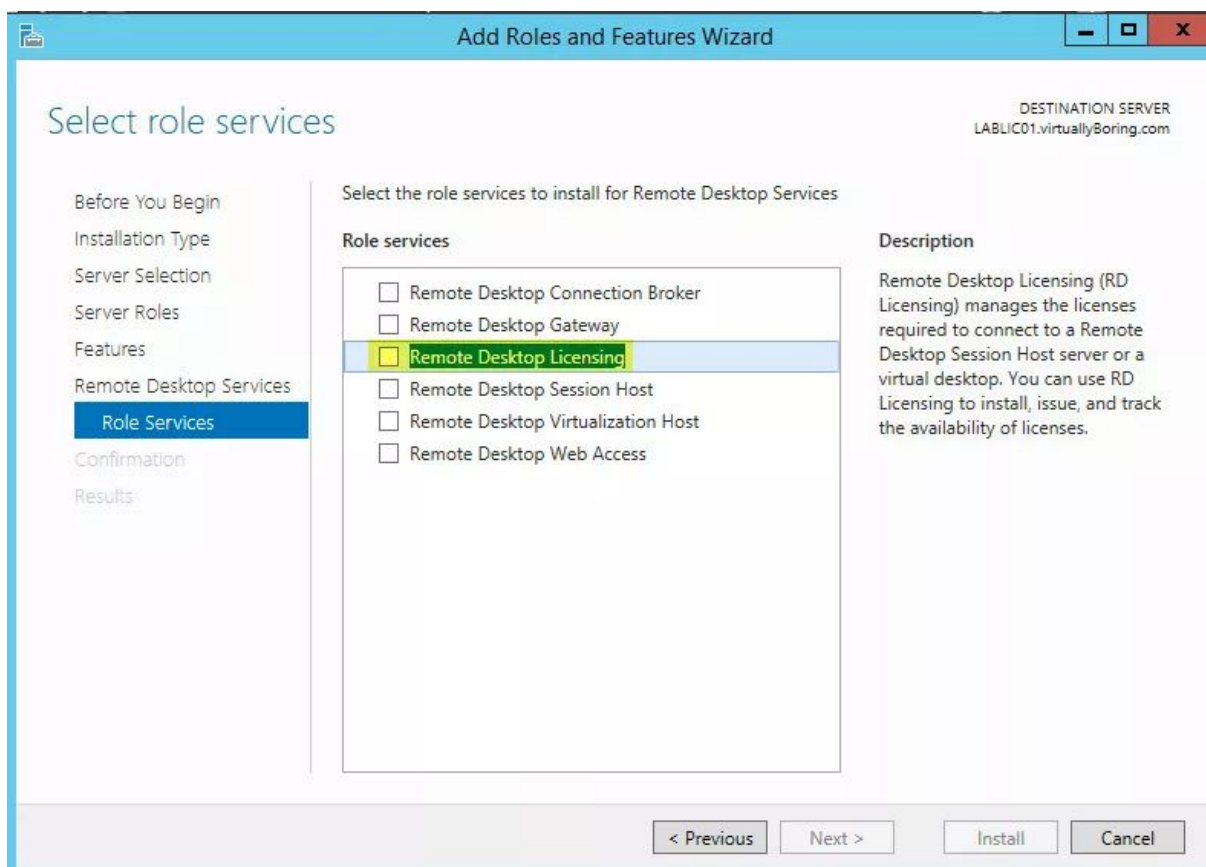


Clickear en Next.





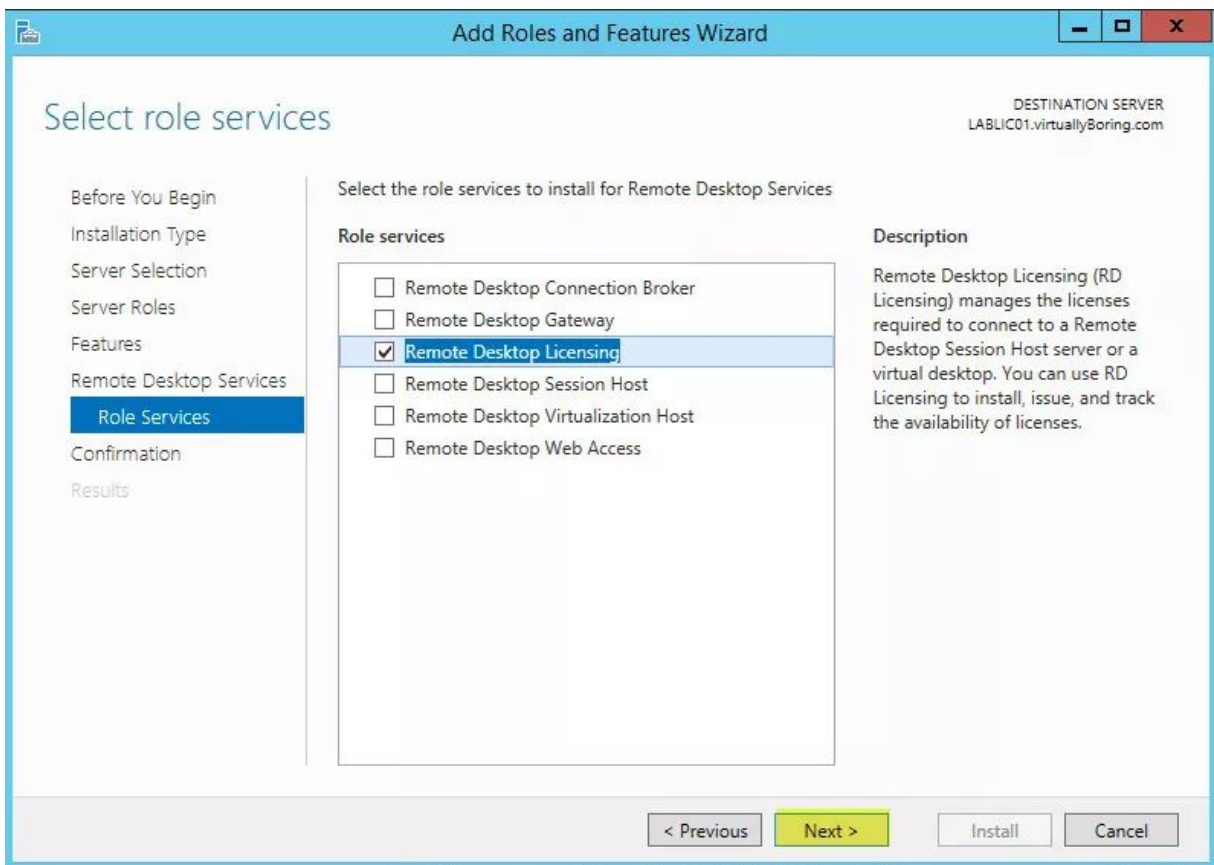
Seleccionar el Rol que se desea instalar.



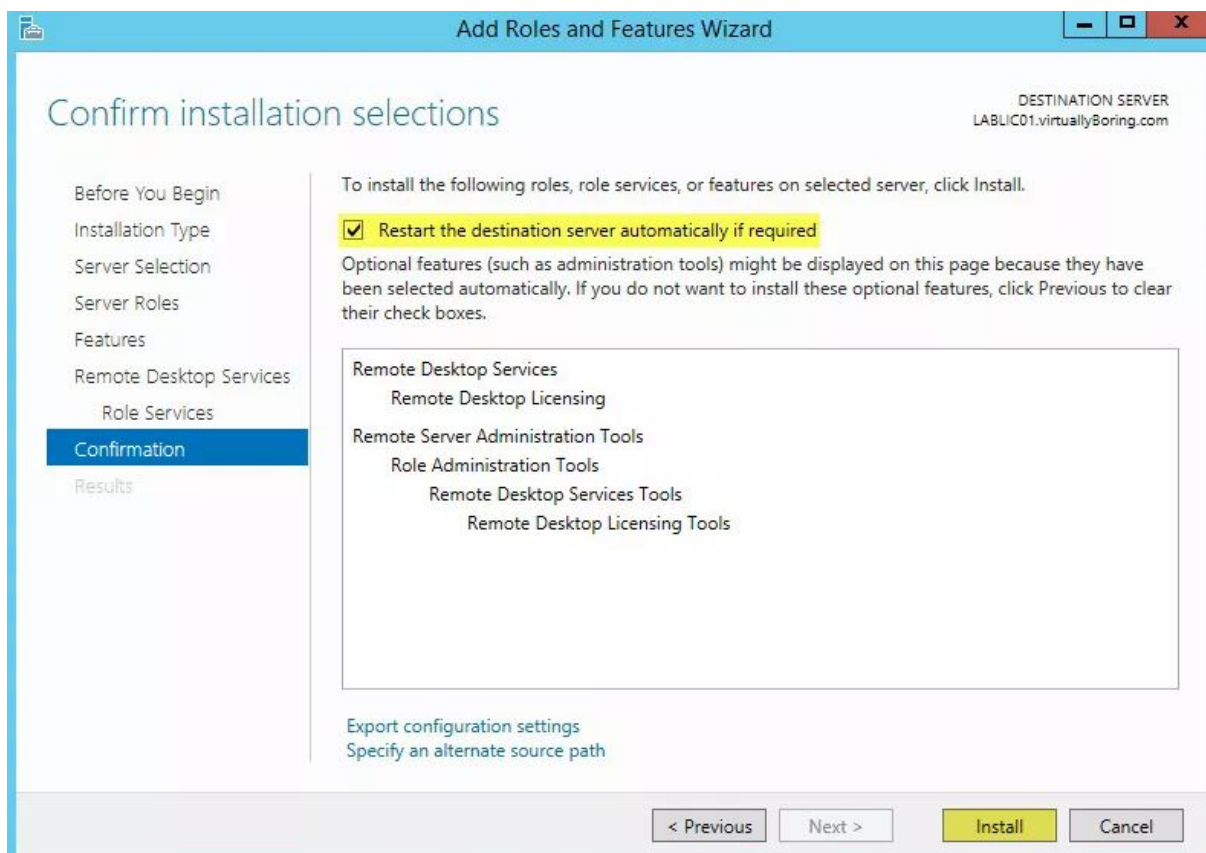
Se debe seleccionar el rol correspondiente según el servidor en el cual se esté trabajando. Los roles de RDSH, RDWA y RDCB desde aquí sin requerir pasos extras. El rol de RDL requiere una configuración posterior a su instalación.

### **Instalación y configuración de RDL**

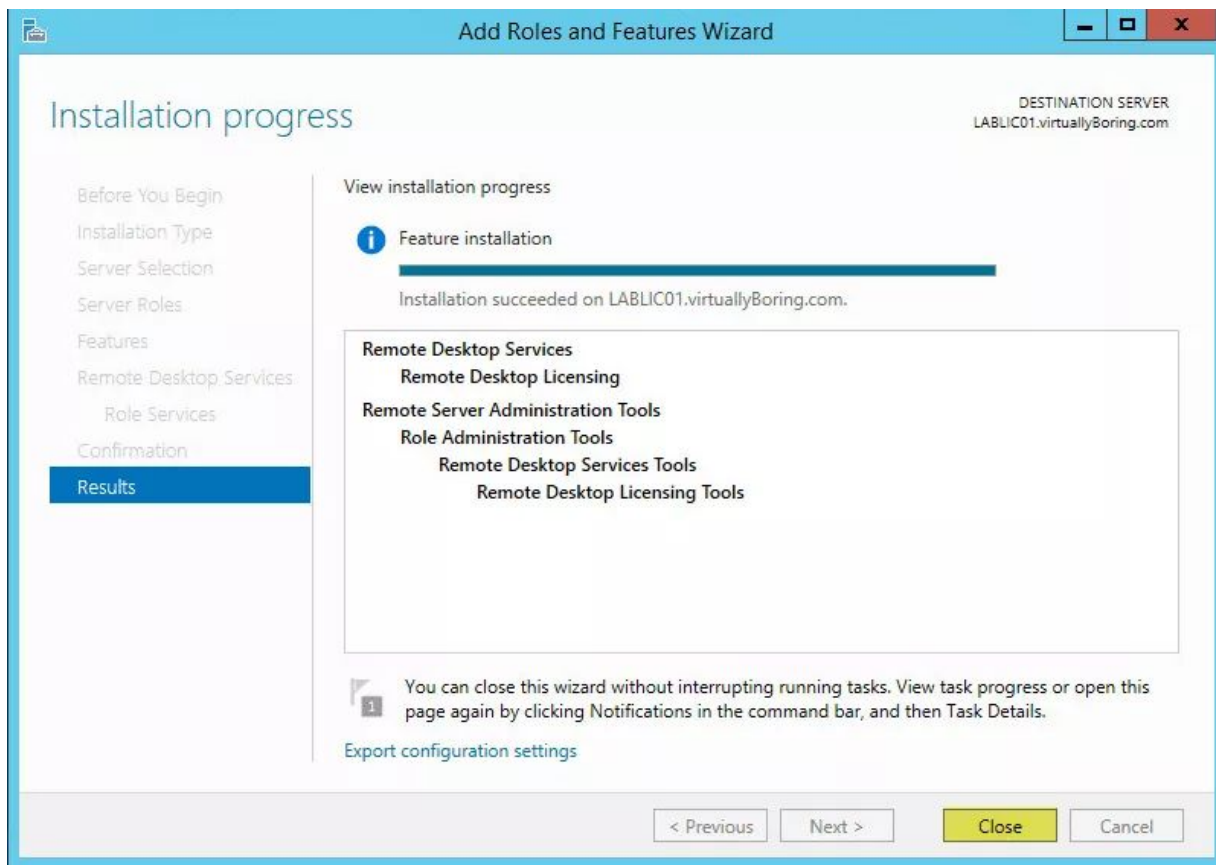
Seleccionar Remote Desktop Licensing y clicar en Next.



Seleccionar Restart the destination server automatically if required , luego clicar en Install.



Cuando finalice clickear en Close.



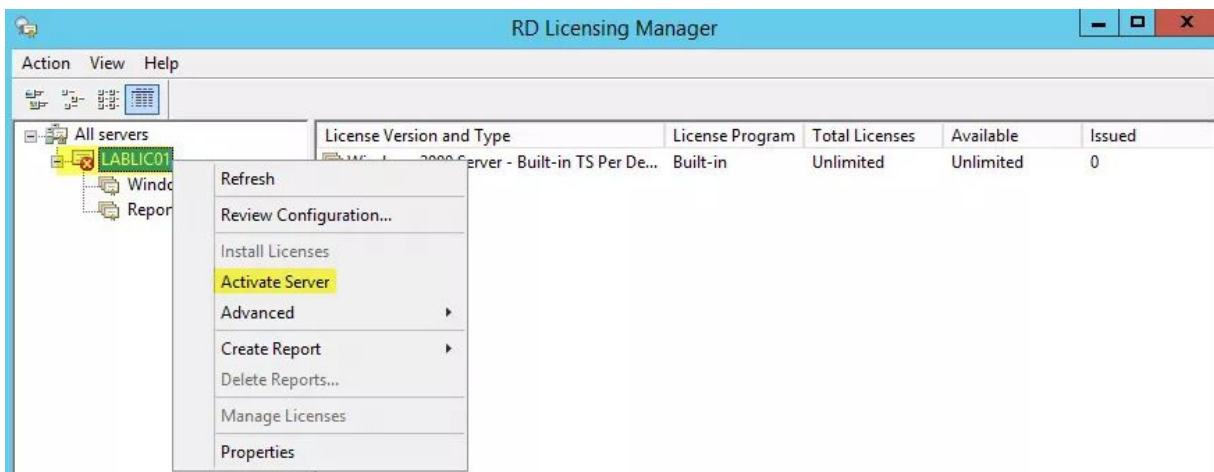
## Activación de RDL

Ahora que el rol de Licenciamiento RD está instalado, necesitamos activarlo con Microsoft. Para hacer esto necesitamos iniciar el Administrador de licencias de escritorio remoto.

Ir a Start -> Control Panel -> Administrative Tools -> Remote Desktop Services-> Remote Desktop Licensing Manager.



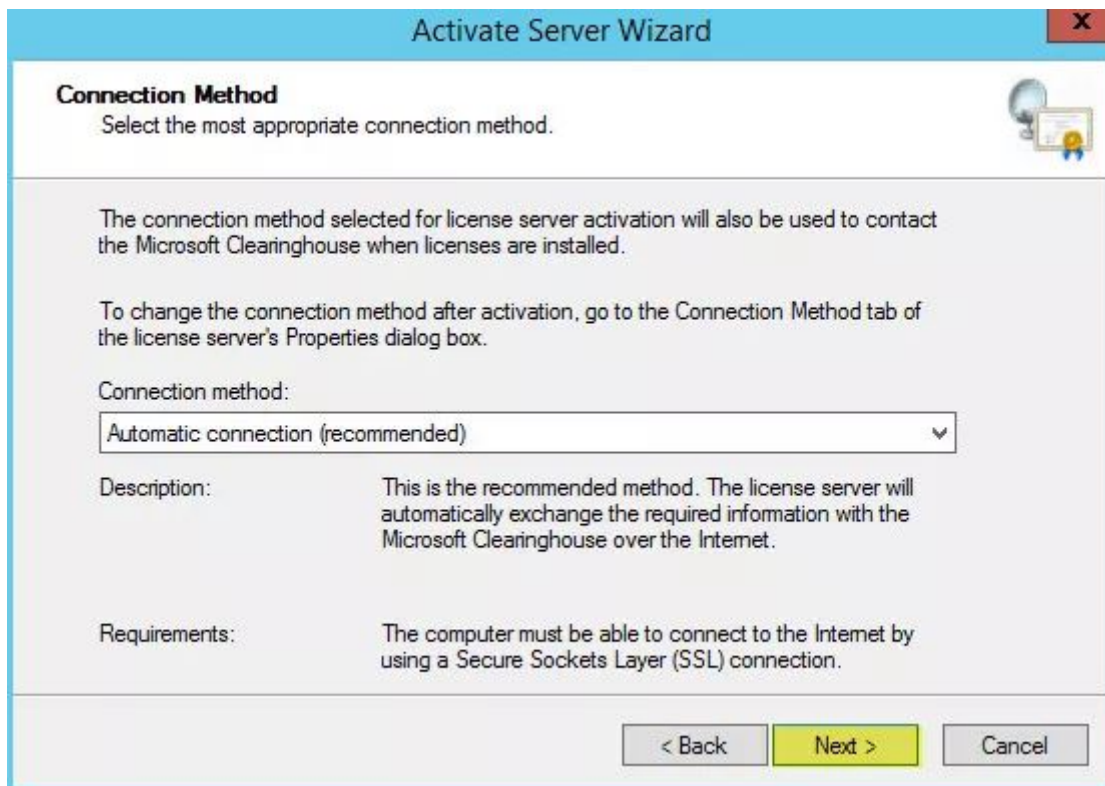
Click derecho en el nombre del servidor y luego click en Activate Server.



Clickear en Next.




Si el servidor está conectado a internet, dejar la opción Automatic connection y clickear en Next.



Ingresa tu información y clickear en Next.

**Activate Server Wizard** X

---

**Company Information**   
Provide the requested company information.

---

Enter your name, company name, and country/region information.  
This information is required to proceed.


First name:

Last name:

Company:

Country or Region:  ▼

---

 Name and company information is used only by Microsoft to help you if you need assistance. Country/Region is required to comply with United States export restrictions.


---

Opcional. Ingresar información adicional y clickear en Next.



**Activate Server Wizard** X

---

**Company Information**  
Enter this optional information. 

Email:


Organizational unit:

Company address:

City:

State/province:

Postal code:

 If provided, the optional information entered on this page will only be used by Microsoft support professionals to help you if you need assistance.

Tildar Start Install Licenses Wizard y clickear en Next.

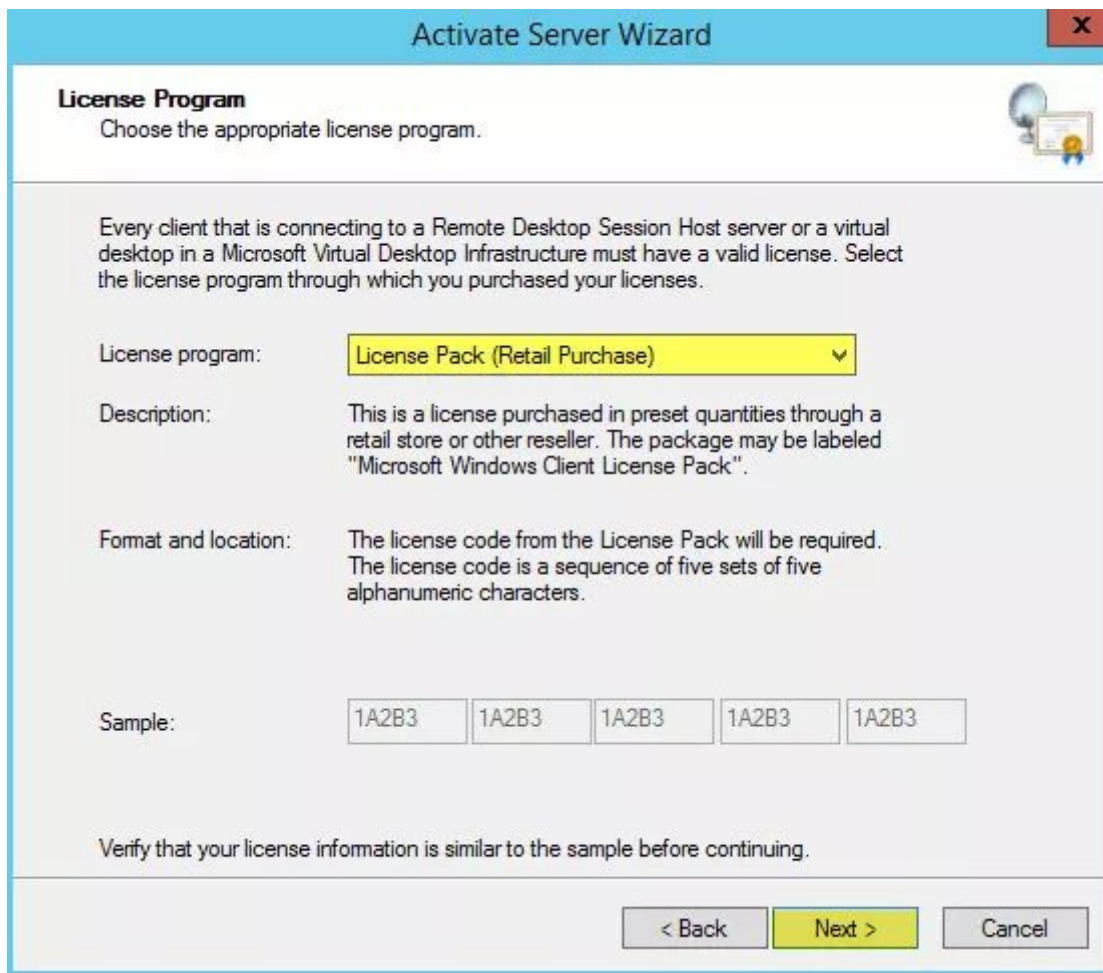


## Instalación de Licencias

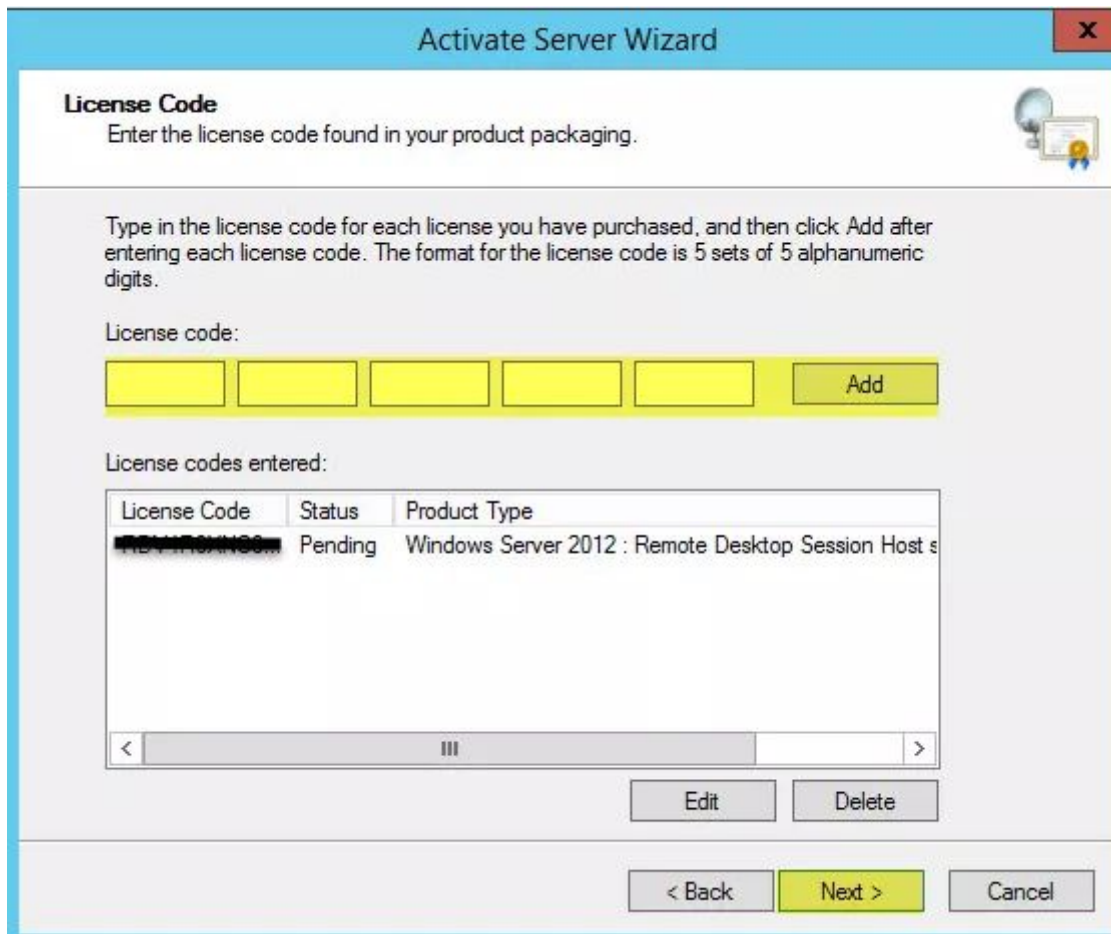
Clickear en Next.



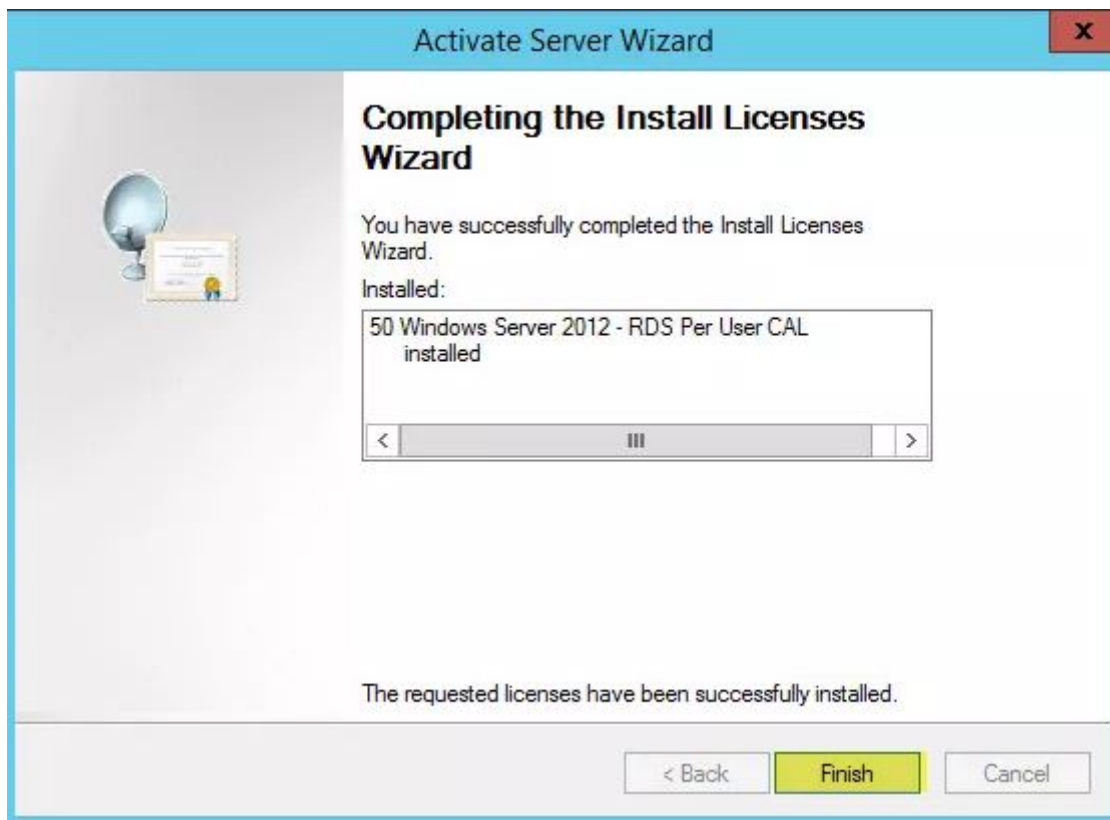
Elegir el tipo de licencia a instalar y clicar en Next.



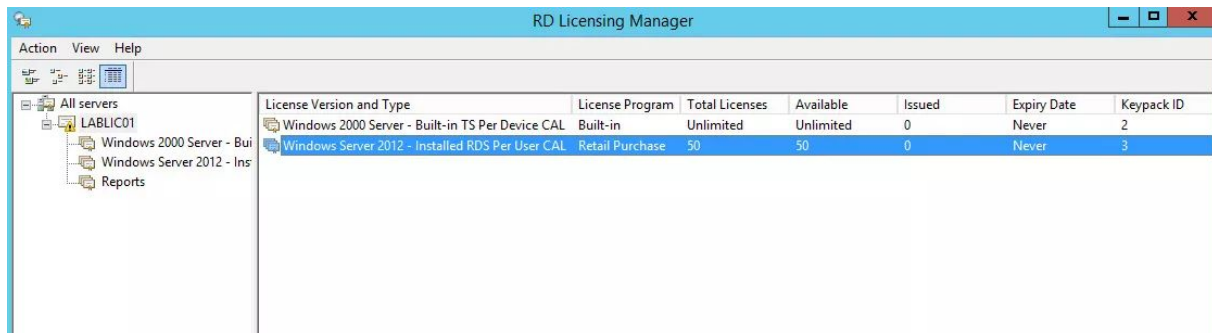
Ingresar la licencia, clickear en Add y luego en Next.



Clickear en Finish para terminar la instalación de la licencia.

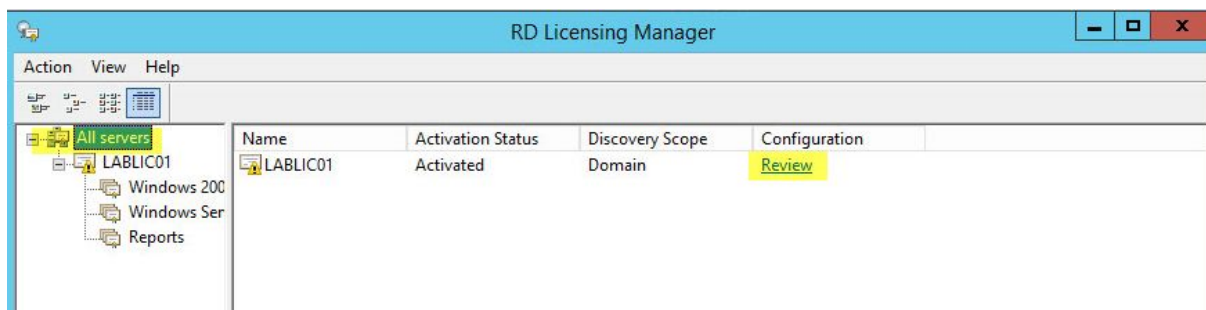


La licencia agregada se mostrará.

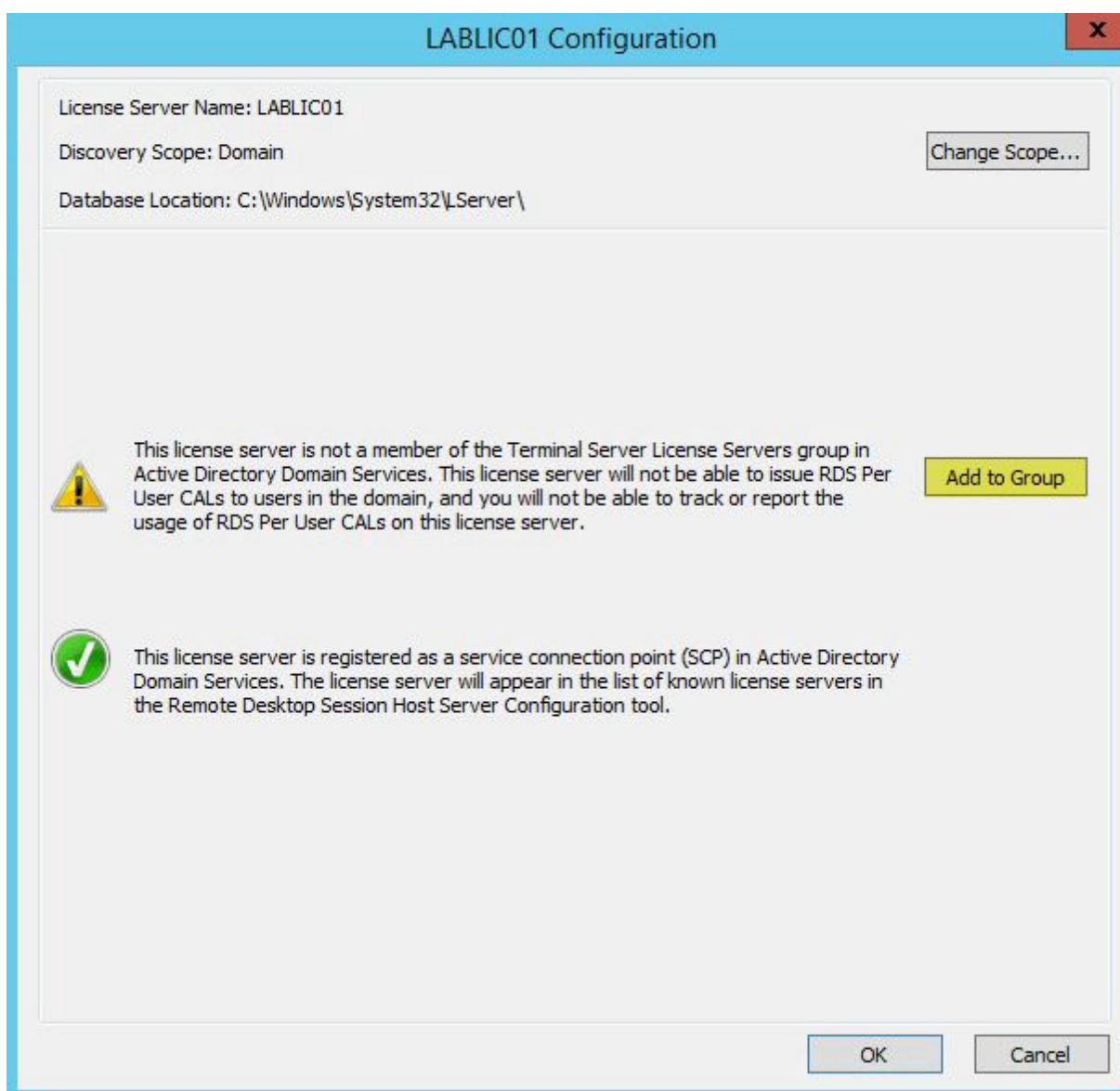


### Agregar el servidor de licencias a Active Directory

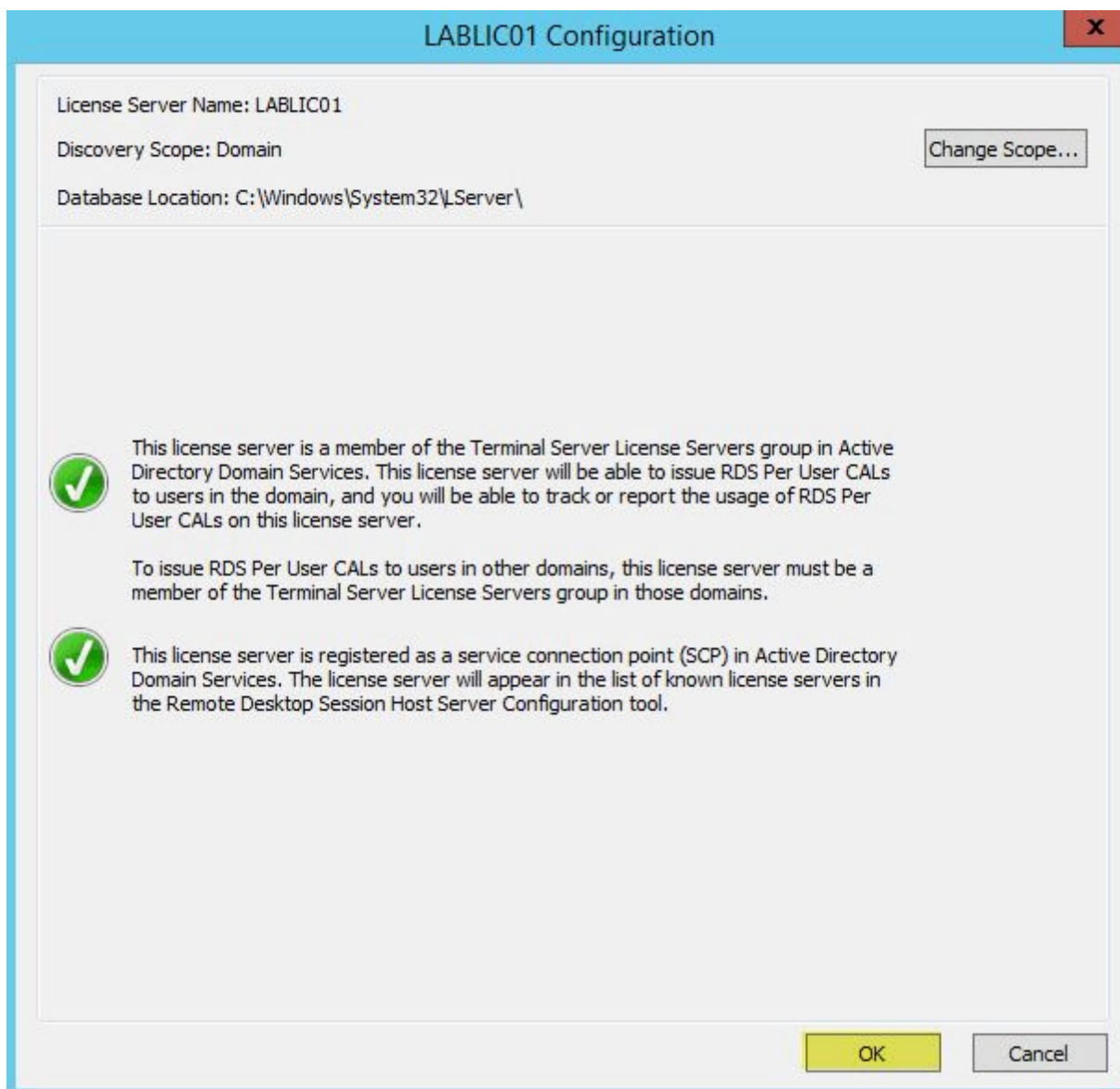
Podemos arreglar el símbolo amarillo junto al nombre de su servidor de licencias. Haga clic en All Servers y luego haga clic en Review.



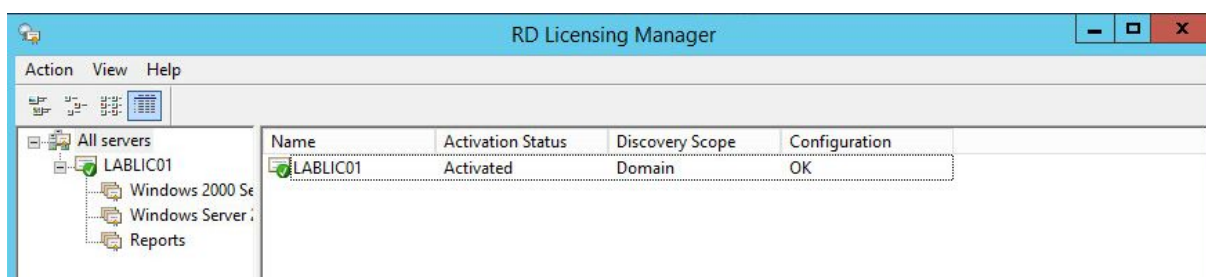
Clickear en Add to Group



Clickear en Ok



La configuración ahora debería aparecer en verde con una marca verde al lado del nombre de su servidor.





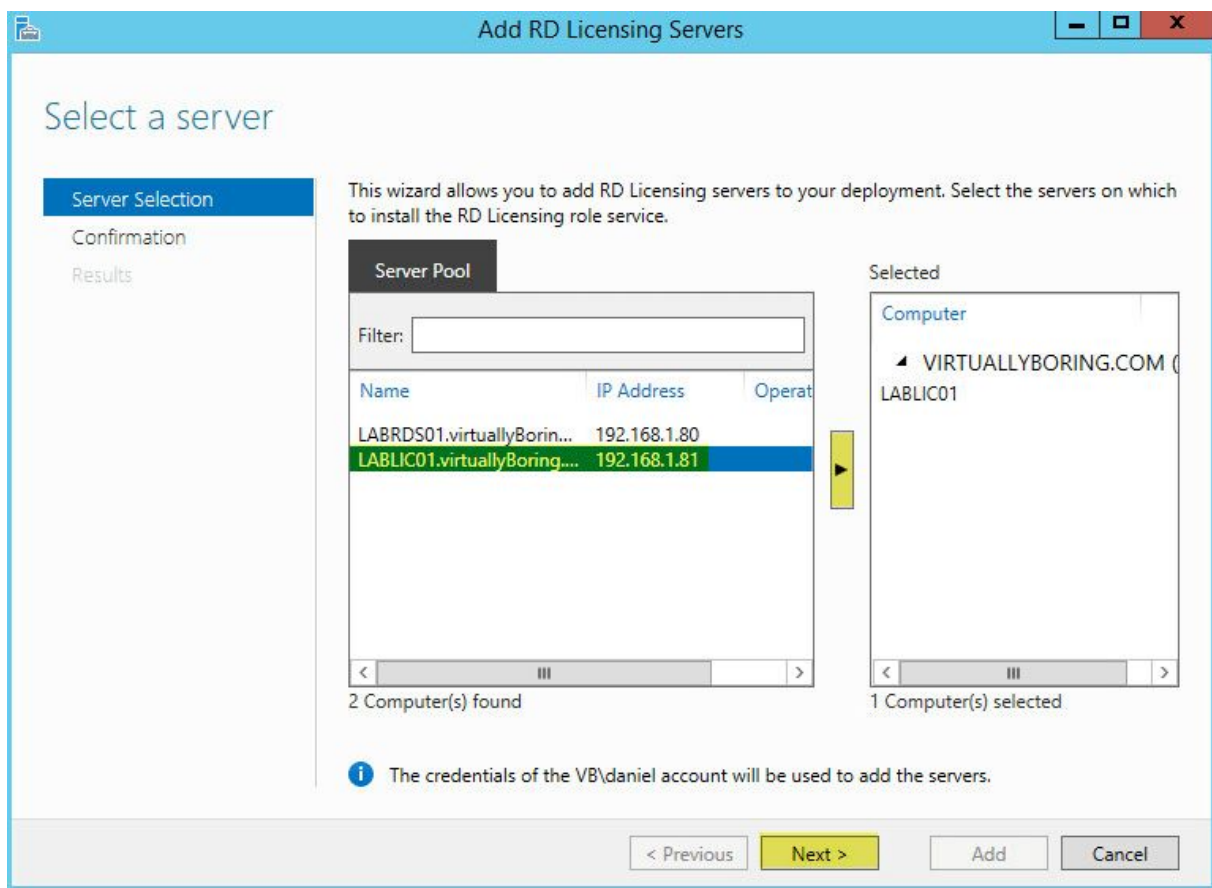
## Agregar el servidor de licencias al entorno RDS

Desde uno de sus servidores RDS abra el Administrador del servidor. Clickear en Remote Desktop Services ->RD Licensing

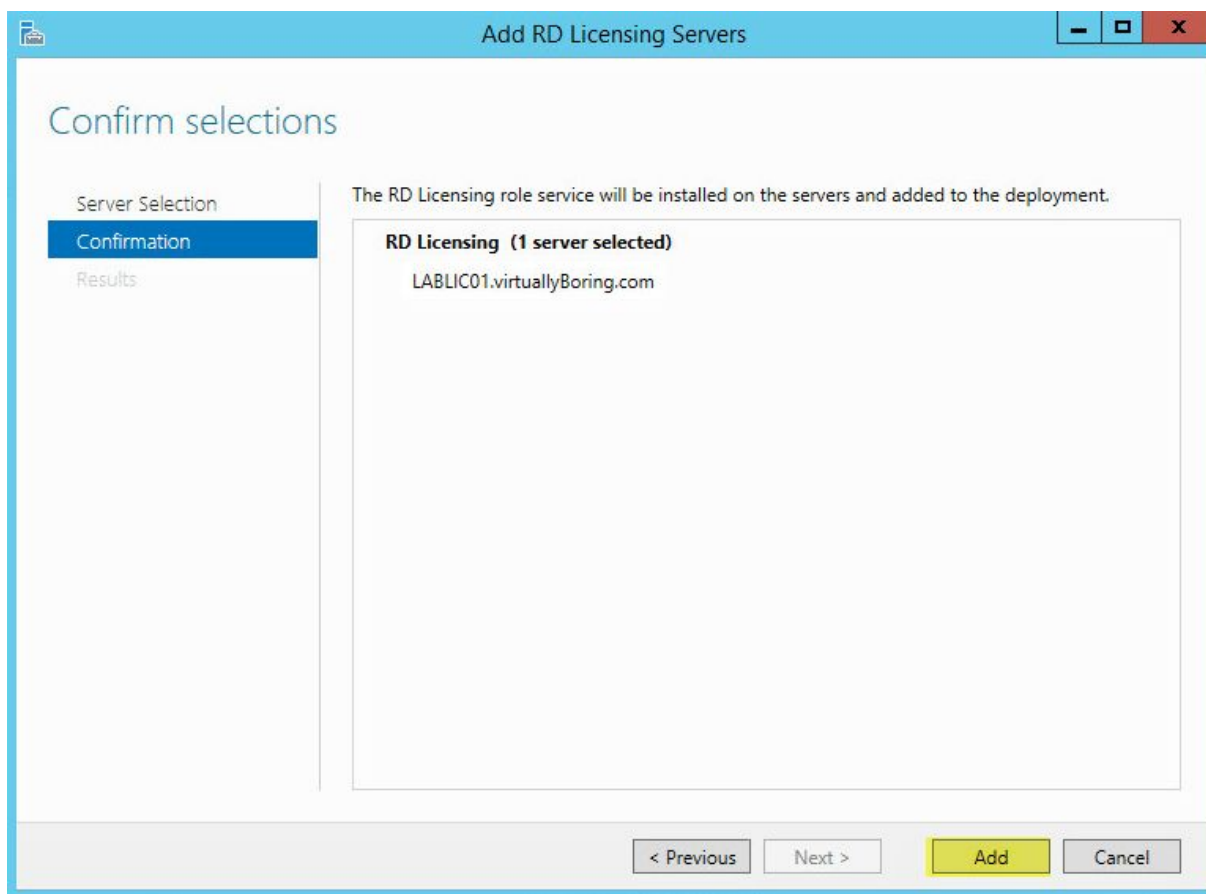
The screenshot displays the Server Manager interface for Remote Desktop Services. The main area shows a deployment overview diagram with components: RD Web Access, RD Gateway, RD Licensing (highlighted), RD Connection Broker, RD Virtualization Host, and RD Session Host. A 'DEPLOYMENT SERVERS' table lists installed role services on the server LABRDS01.VIRTUALLYBORING.COM.

Server FQDN	Installed Role Service
LABRDS01.VIRTUALLYBORING.COM	RD Connection Broke
LABRDS01.VIRTUALLYBORING.COM	RD Session Host
LABRDS01.VIRTUALLYBORING.COM	RD Web Access

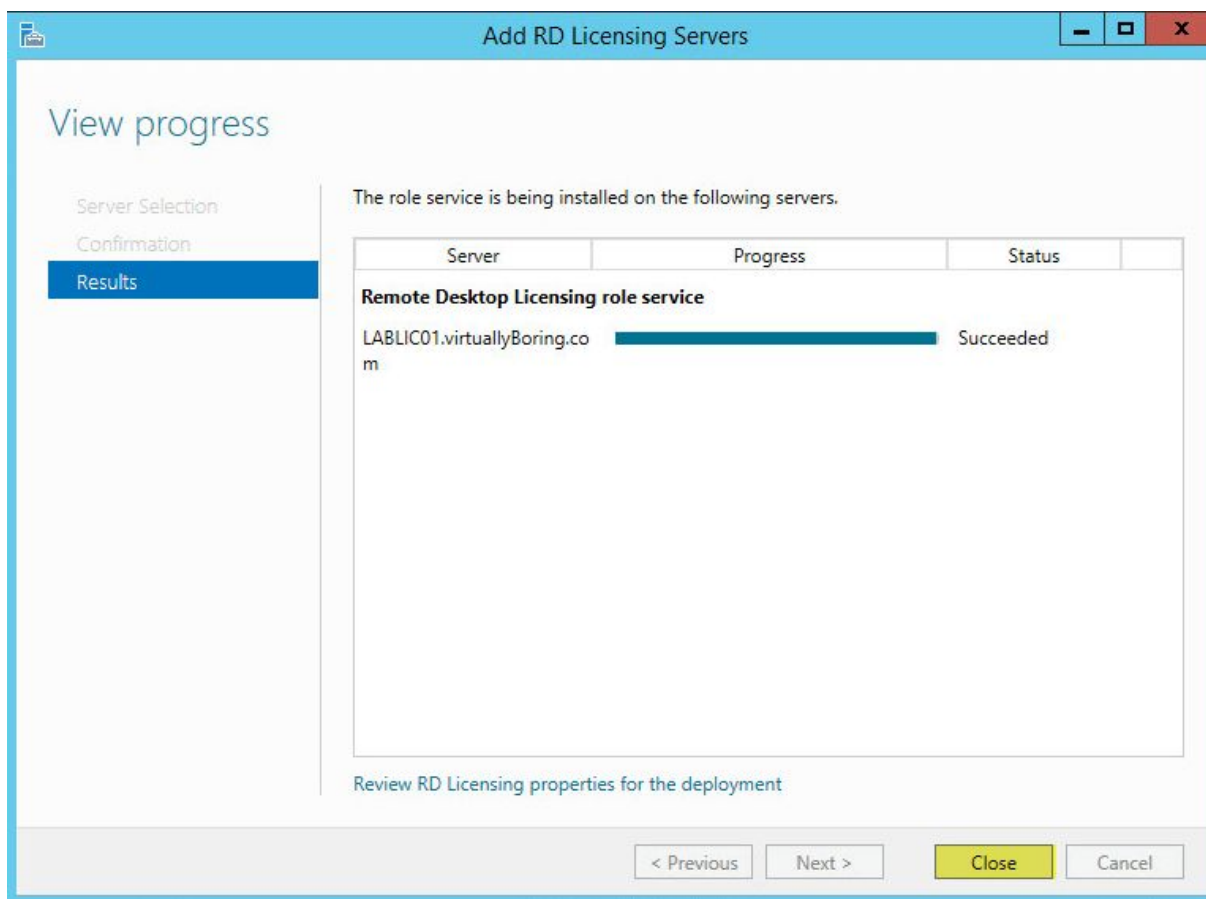
Seleccionar el servidor RDL, clickear en la flecha y luego en Next.



Clickear en Add.



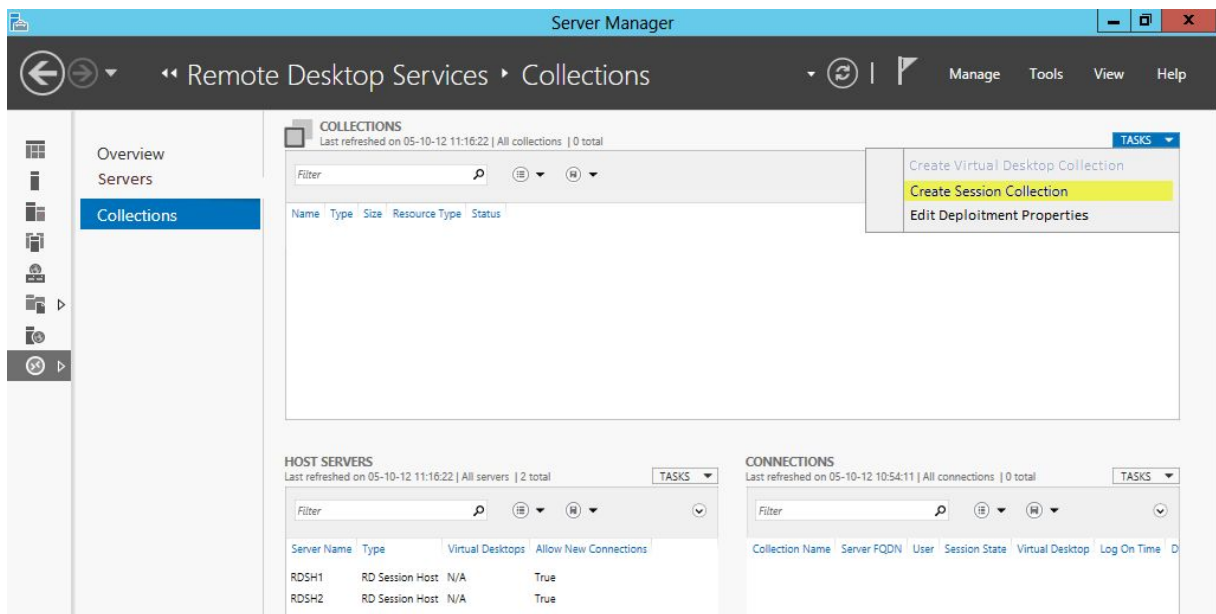
Cuando finalice clickear en Close.



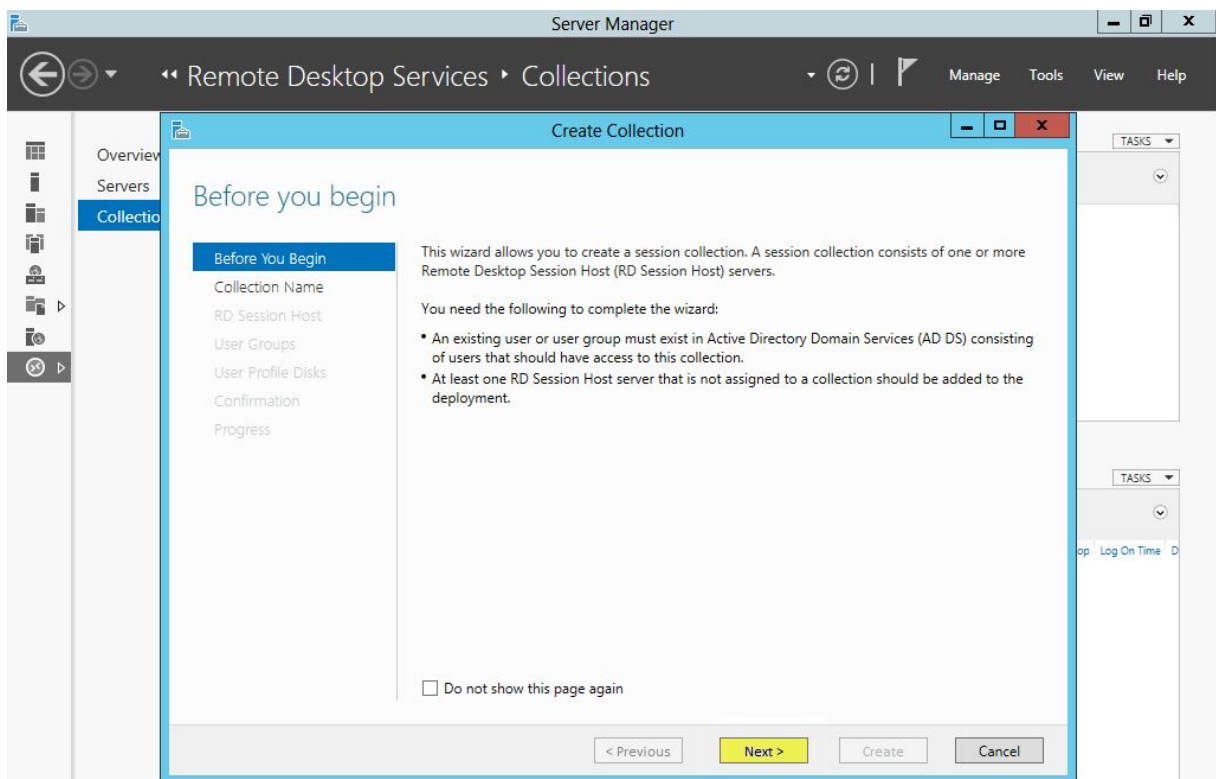
## Publicación de aplicaciones

Una colección es una agrupación lógica de servidores RDSH desde la que se puede publicar la aplicación. Nota: Cada servidor RDSH solo puede participar en una única colección.

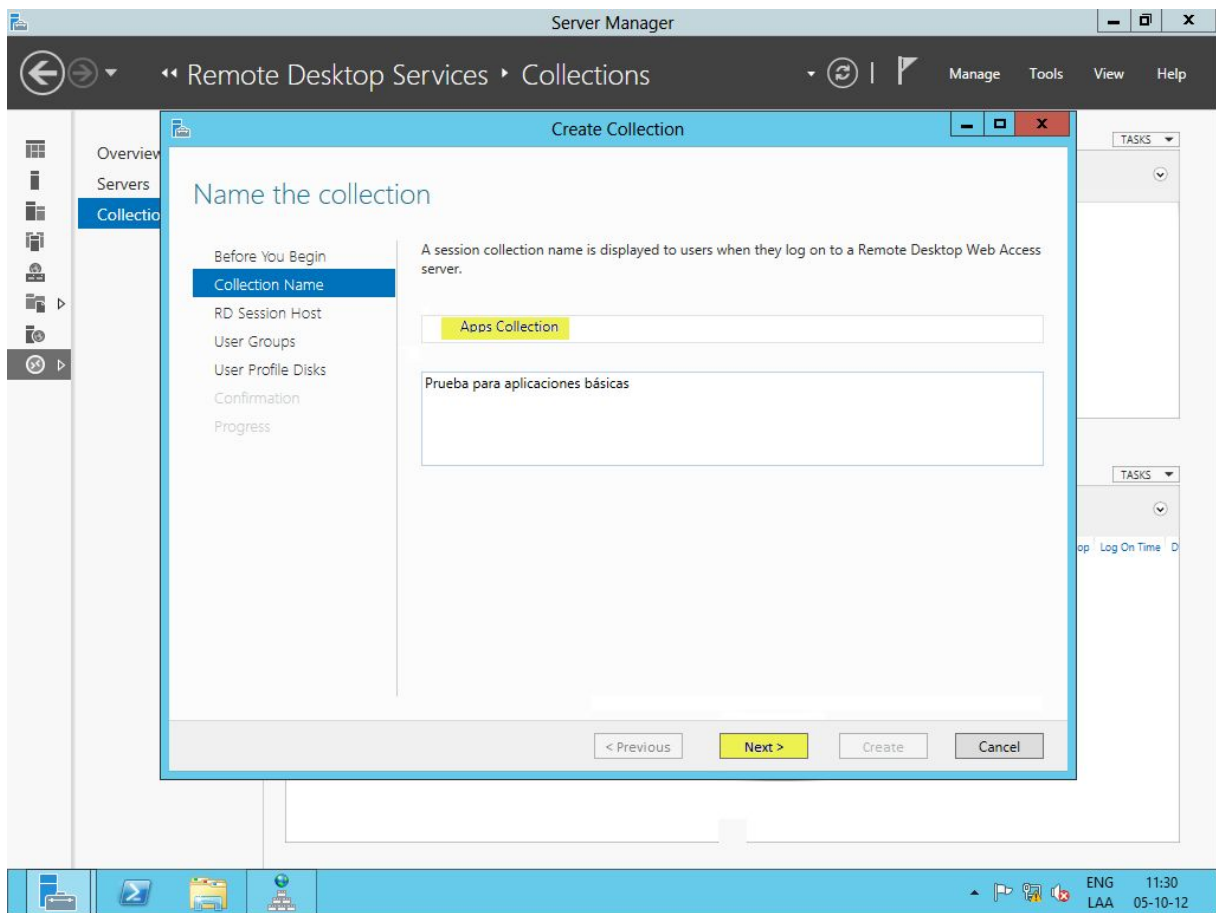
Para poder publicar aplicaciones (RemoteApp) debemos primero crear la Session Collection.



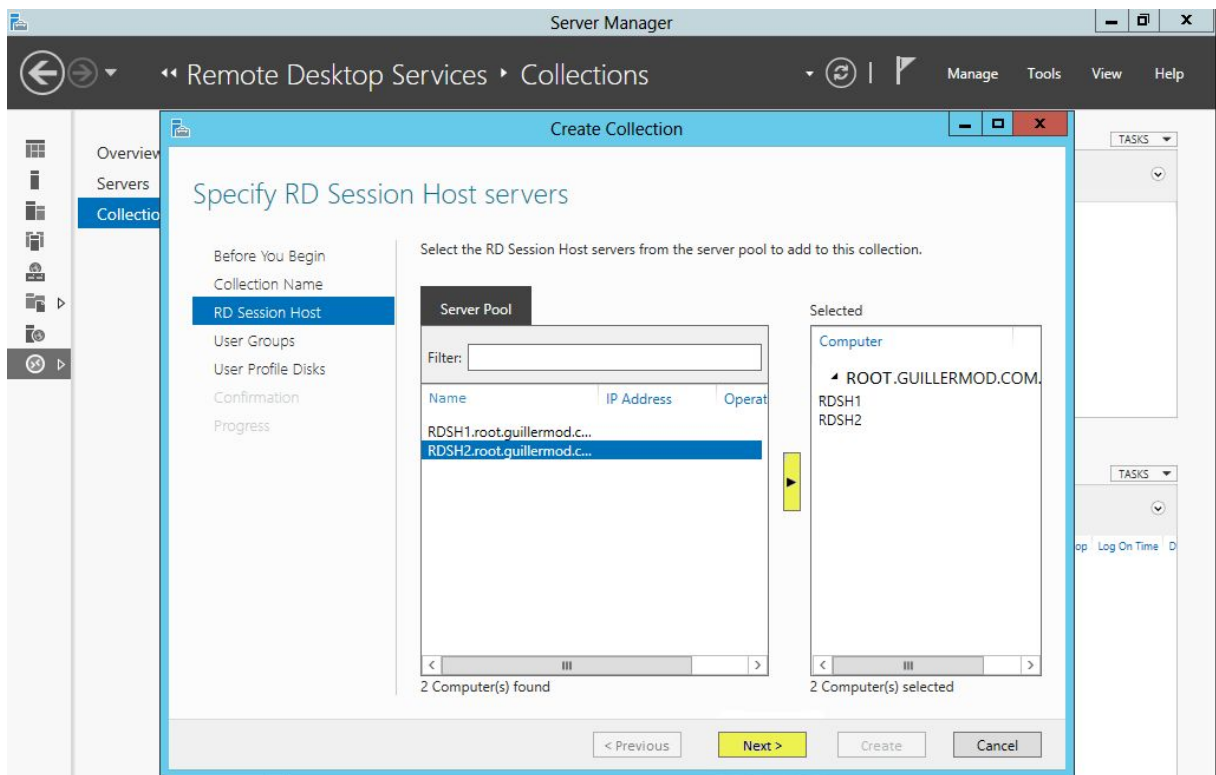
Clicar en Next.



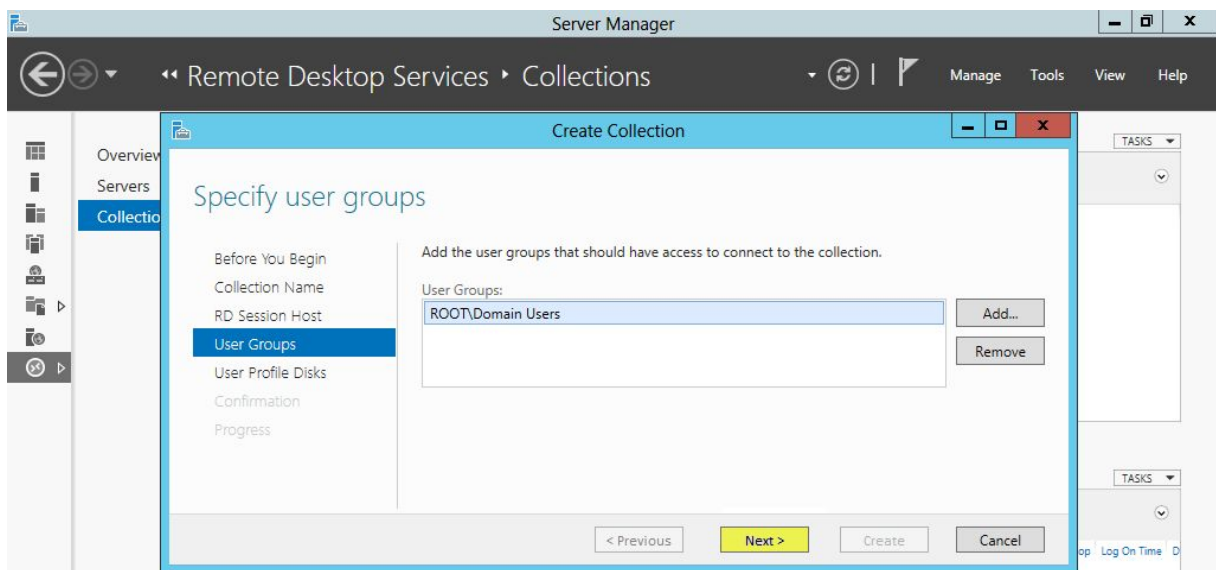
Introducir un nombre para la colección y clicar en Next.



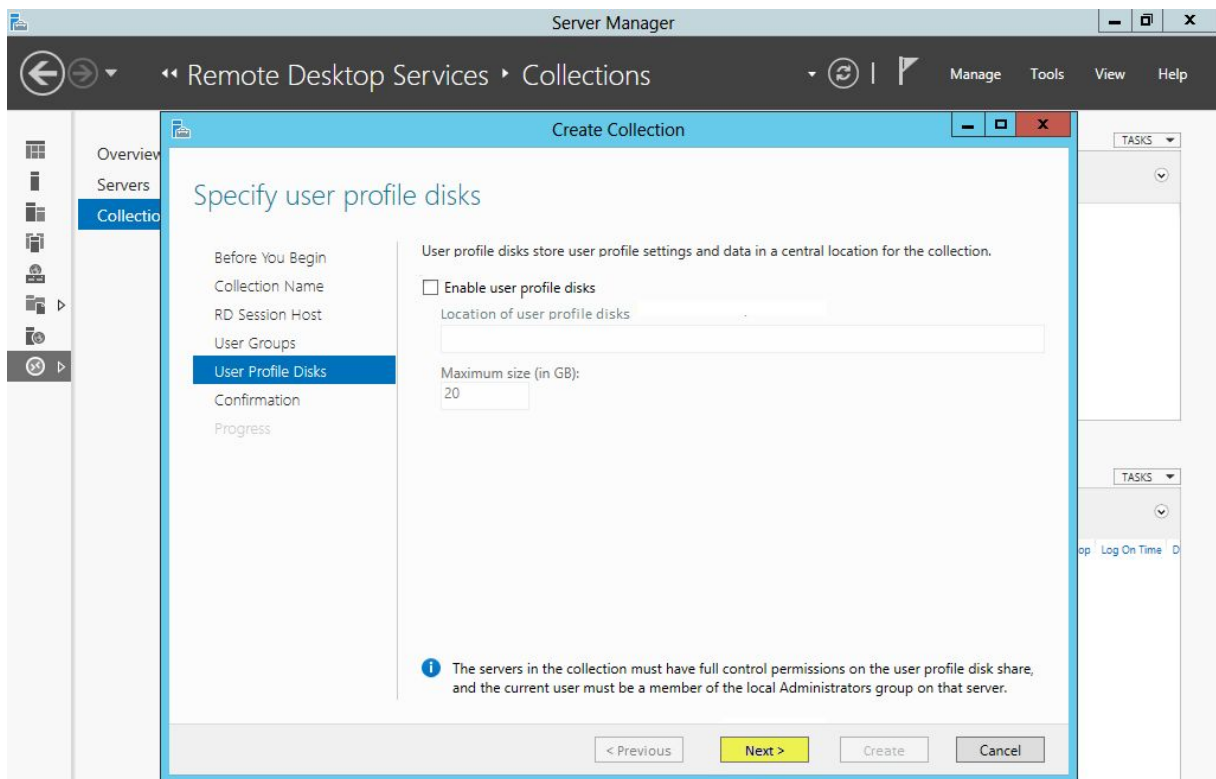
Seleccionar los RDSH donde estarán las aplicaciones publicadas y clicar en Next.



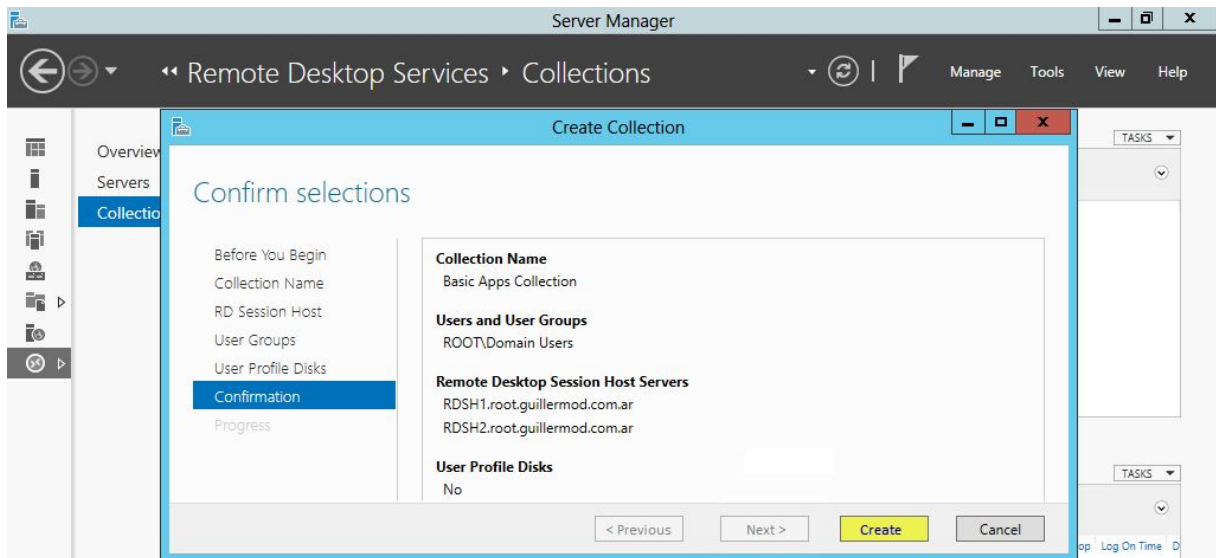
Seleccionar los usuarios y/o grupos que tendrán acceso a la colección y clicar en Next.



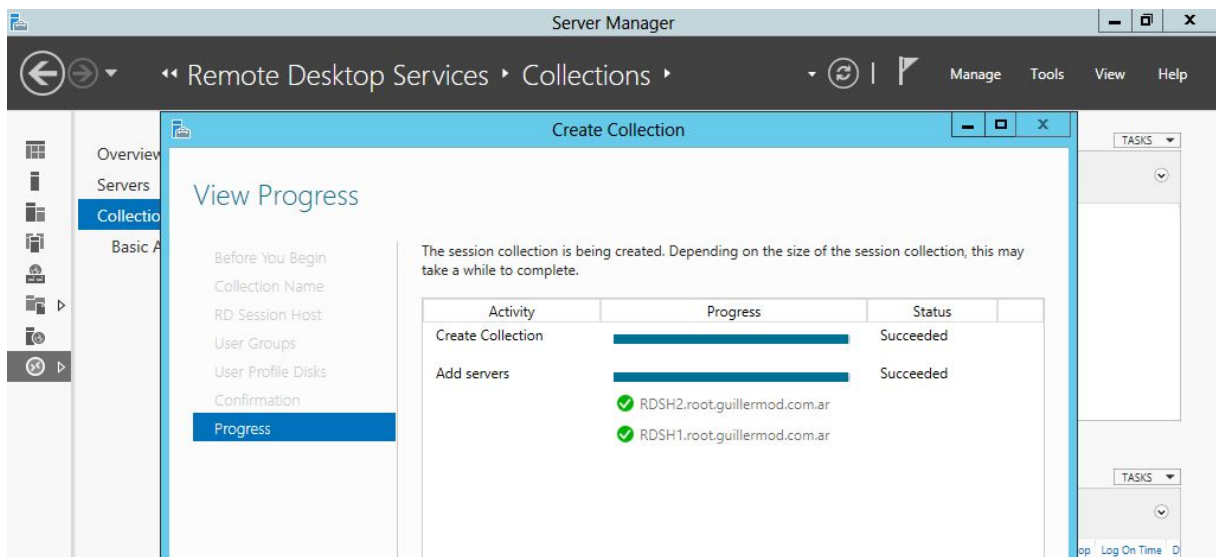
Desmarcar la opción Enable user profile disks and clicar en Next.



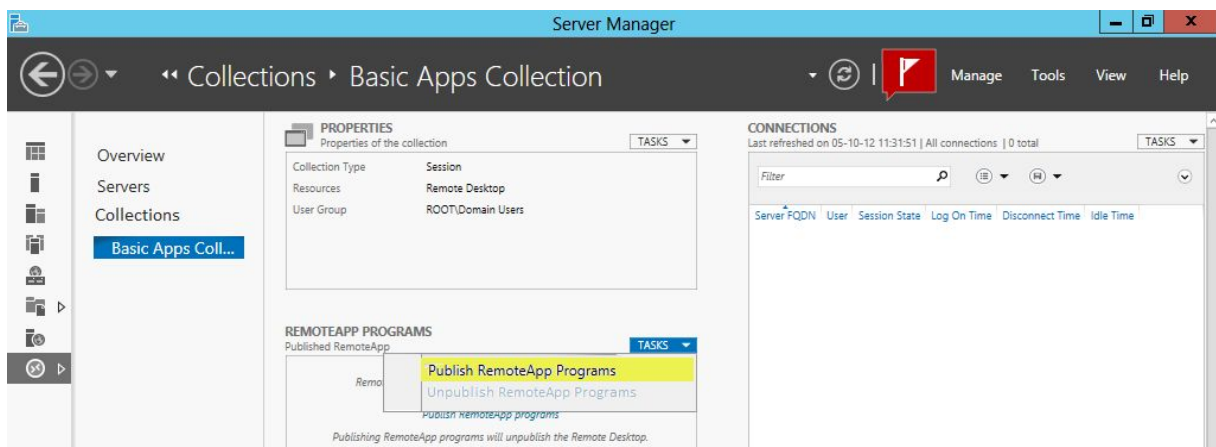
Clickear en Create.



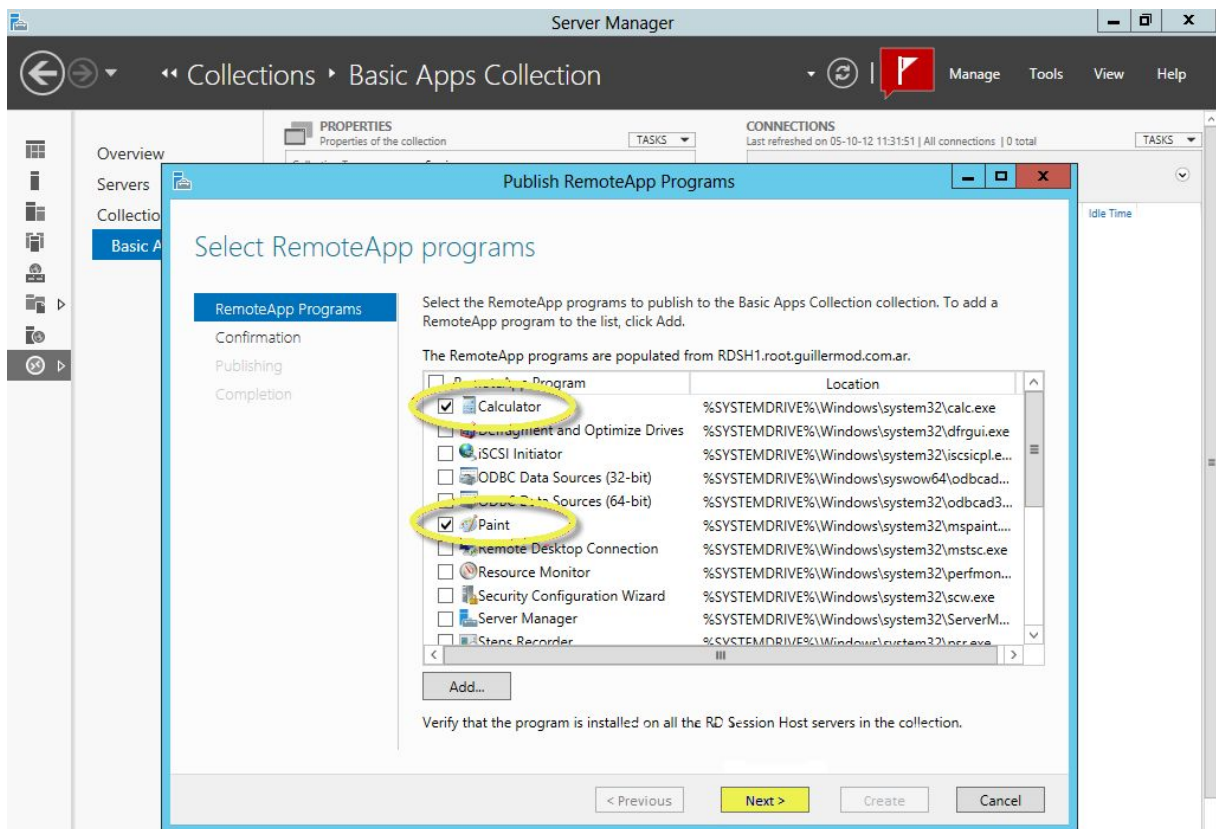




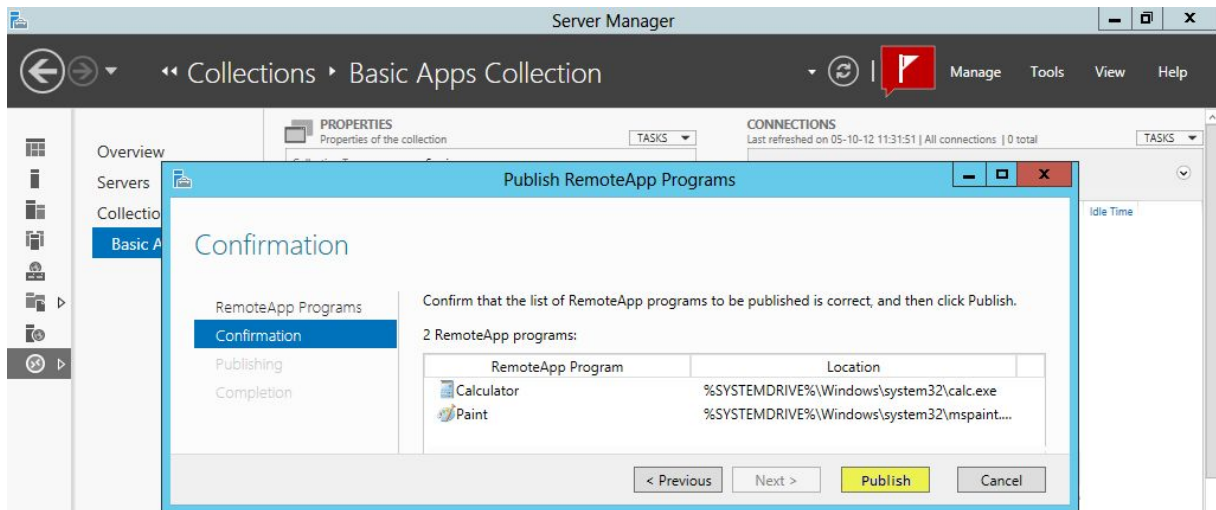
Ahora publicamos las aplicaciones. Clickear en Publish RemoteApp Programs.



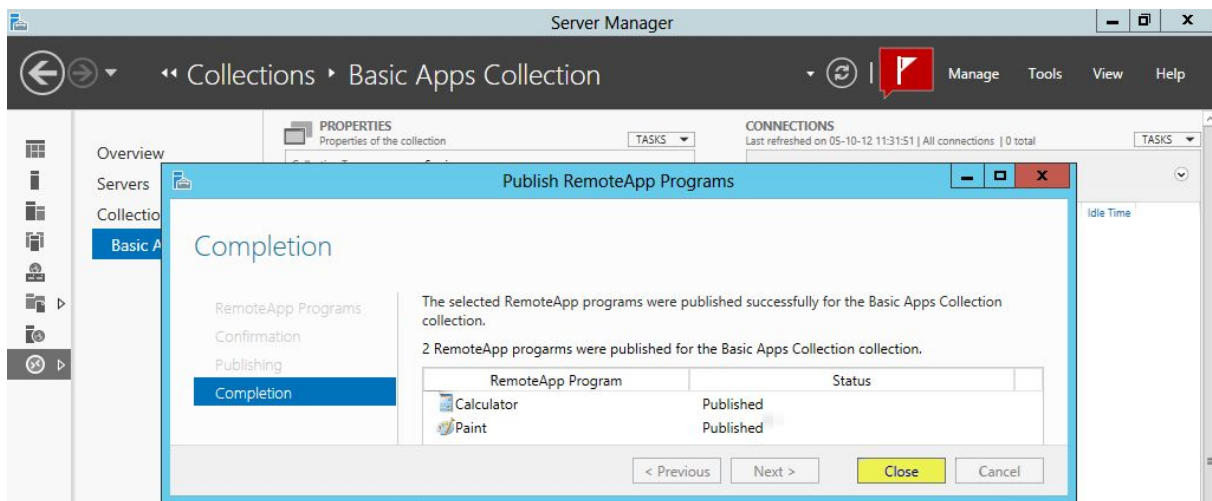
Seleccionar las aplicaciones a publicar y clickear en Next. Tener en cuenta que tienen que estar instaladas en todos los RDSH de la colección.



Clickear en Publish.



Clickear en Close para finalizar la creación de la colección.

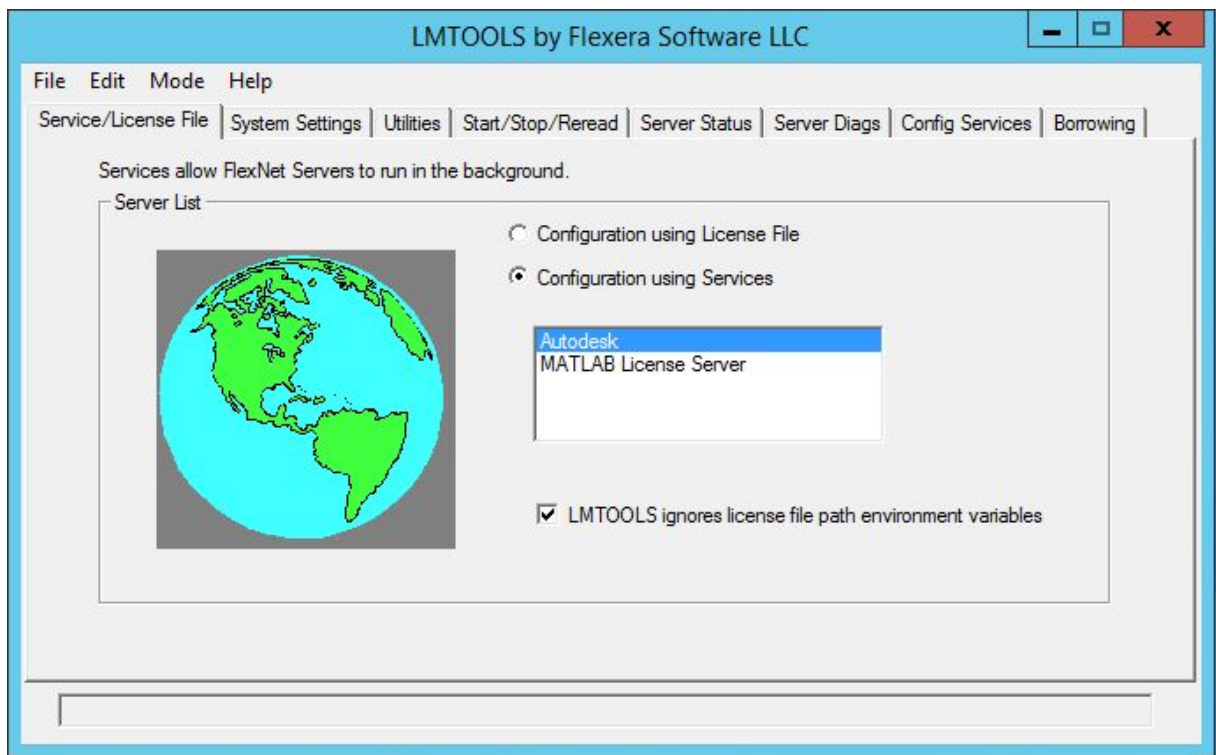


## Configuración de NLM Flexera

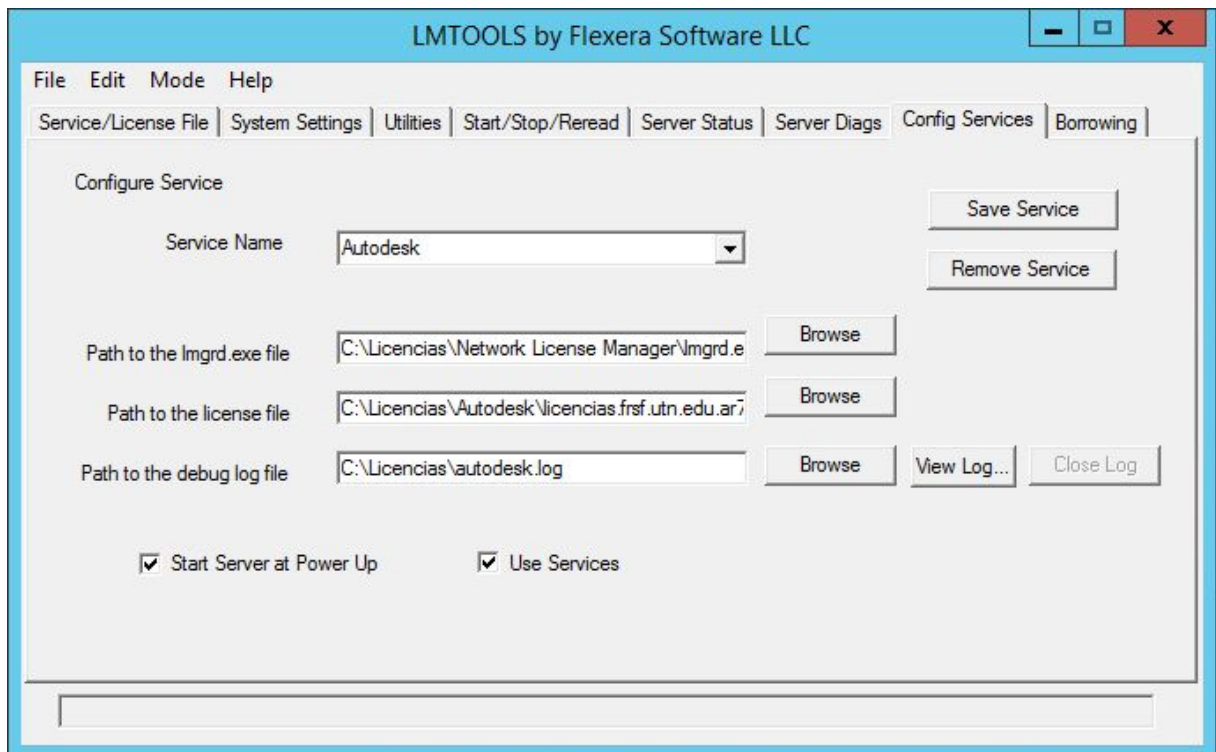
Para el licenciamiento de los software Autocad y Mathlab empleamos el software Lmtools de Flexera y de los daemon específicos de las aplicaciones a licenciar.

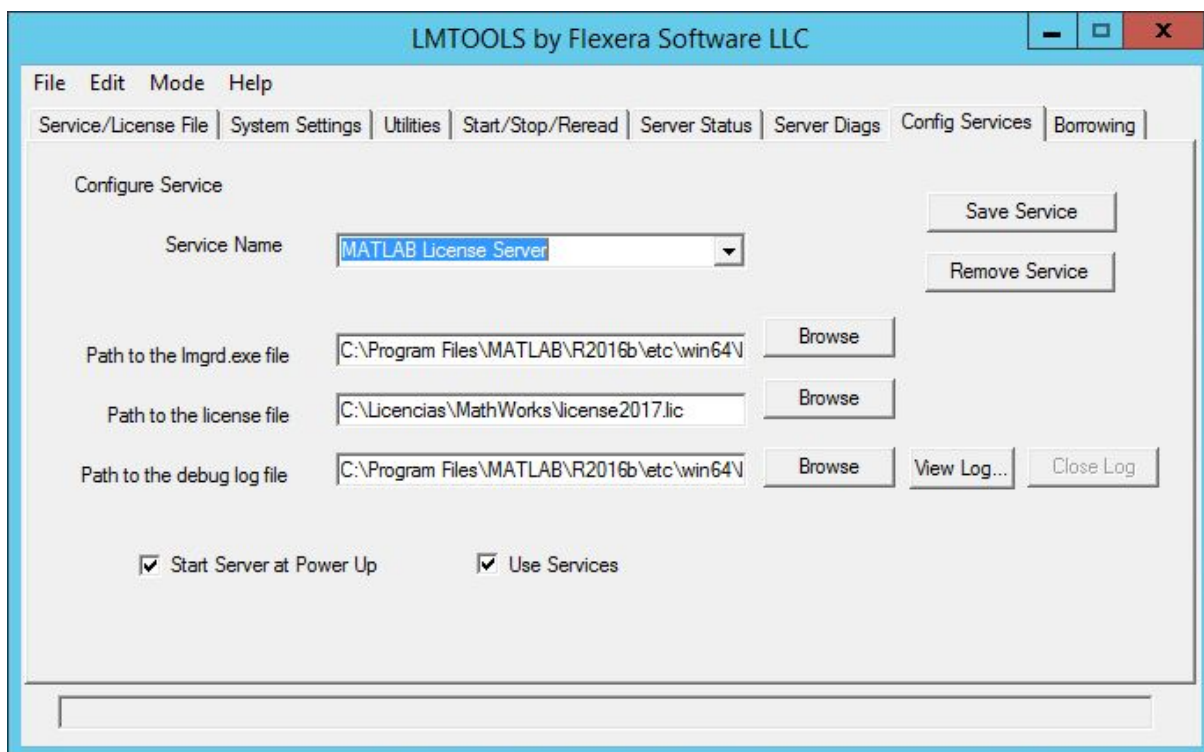
Una vez instalados los daemon y Lmtools debemos ejecutarlo para realizar las configuraciones siguientes:

1. En la pestaña **Service/License File**, seleccionar el modo de configuración usando servicios.

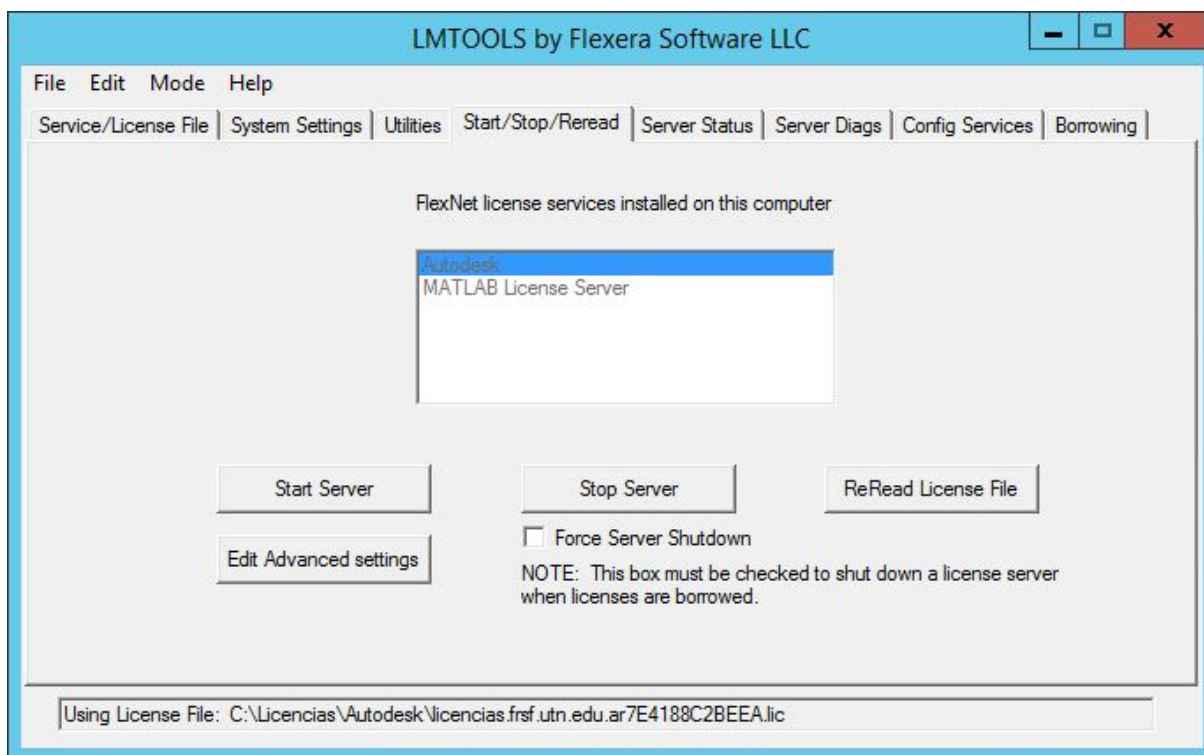


2. En la pestaña **Config Services**, para cada aplicación, ingresar la ubicación del archivo `lmrgd.exe`, la ubicación del archivo de licencia `.lic` y la ubicación del archivo de logs para debug. Tildar las casilla **Start Server at Power Up** y **Use Services**.





3. La pestaña **Start/Stop/Reread** nos permite iniciar o detener el servicio de licenciamiento de cada software y también permite releer el archivo de licencias en caso de que se haya cambiado.



## Implementación de Rol de AD en Windows Server

1. Añadir el rol de servicios de dominio de Active Directory.
  - a. Iniciar Administrador del Servidor.
  - b. Clickear en **Agregar roles y características**.
  - c. En la página Antes de empezar, clickear en **Siguiente**.
  - d. Para el tipo de instalación, seleccionar **Instalación basada en características o en roles** y, a continuación, clickear en **Siguiente**.
  - e. Seleccionar la opción **Seleccionar un servidor del grupo de servidores** y, a continuación, seleccionar el servidor local de la lista Agrupación de servidores. Clickear **Siguiente**.
  - f. En la lista Roles, seleccionar **Servicios de dominio de Active Directory**.
  - g. Clickear en **Agregar características**.
  - h. Clickear en **Siguiente**.
  - i. En la página Seleccionar características, aceptar los valores predeterminados y clickear en **Siguiente**.
  - j. En la página de confirmación, clickear en **Instalar**.
  - k. Clickear en **Cerrar** una vez concluida la instalación y, a continuación, reiniciar el servidor.
2. Promocionar el servidor a un controlador de dominio.
  - a. Iniciar Administrador del Servidor.
  - b. Clickear en **AD DS** en el panel de instrumentos.
  - c. Clickear en el indicador de advertencia **Configuración necesaria para servicios de dominio de Active Directory**.
  - d. En la página Todos los detalles y notificaciones de tareas de servidor, clickear en la acción **Promover este servidor a un controlador de dominio**.
  - e. En la página Configuración de implementación, seleccionar **Agregar un nuevo bosque**. Especificar el nombre de dominio raíz con un nombre de dominio exclusivo totalmente calificado, en nuestro caso, FRSF.UTN.EDU.AR y, a continuación, clickear en **Siguiente**.

- f. En la página Opciones de controlador de dominio, desmarcar la opción **Servidor de sistema de nombres de dominio (DNS)**, y proporcionar una contraseña para el Modo de restauración de servicios de directorio (DSRM). Clickear en **Siguiente**.
- g. Aceptar el nombre NetBIOS predeterminado y clickear en **Siguiente**.
- h. Aceptar las Rutas de acceso predeterminadas para la base de datos **AD DS**, los archivos de registro y SYSVOL. Clickear en **Siguiente**.
- i. Revisar el resumen, clickear en **Siguiente** y, a continuación, clickear en **Instalar**.
- j. Reiniciar el servidor

Cuando se reinicie el servidor, incluya el dominio que ha especificado con las credenciales de inicio de sesión. En este ejemplo, se ha creado un dominio FRSF. Especifique FRSF\Administrador como usuario cuando inicie sesión en el sistema.

### **Creación de contenedores, usuarios y grupos.**

1. Seleccionar **Panel de control > Herramientas administrativas > Usuarios y equipos de Active Directory**.
2. Seleccionar el servidor, clickear con el botón derecho y seleccionar **Nuevo > Unidad organizativa**.
3. Especificar un nombre para la unidad organizativa, por ejemplo, **RDS** y, a continuación, clickear en **Aceptar**.
4. Clickear con el botón derecho en la unidad organizativa **RDS** y clickear en **Nuevo > Usuario**.
5. Crear un usuario denominado **labmovil**. Especificar **Laboratorio** como **Nombre** y **labmovil** como **Nombre de inicio de sesión**. Clickear en **Siguiente**.
6. Proporcionar una contraseña para **labmovil**. Clickear en **Siguiente** y, a continuación, en **Finalizar**.
7. Clickear con el botón derecho en la unidad organizativa **RDS** y seleccionar **Nuevo > Grupo**.

8. Denominar el grupo **LaboratorioMovil** y clicar en **Aceptar**.
9. Clickear con el botón derecho en el grupo **LaboratorioMovil** y seleccionar **Propiedades**.
10. En la ficha **Miembros**, clicar en **Añadir**.
11. Escribir **labmovil** en el campo **Escriba los nombres de objeto que desea seleccionar** y, a continuación, clicar en **Aceptar**. Ahora el usuario **labmovil** es un miembro de la lista de miembros de **LaboratorioMovil**.

## Configuración de Firewall de Windows

La activación y configuración de reglas de Firewall en Windows Server puede realizarse mediante la consola de comandos de PowerShell. A continuación se muestran los comandos básicos de PowerShell para configurar el firewall según las necesidades de nuestra aplicación:

- Activar el Firewall:

```
Set-NetFirewallProfile -Profile Domain,Public,Private  
-Enabled True
```

- Mostrar el estado del Firewall:

```
netsh advfirewall show allprofiles
```

- Crear reglas para permitir conexiones RDP en la infraestructura de virtualización:

- `New-NetFirewallRule -DisplayName "Escritorio remoto - Modo usuario (TCP de entrada)" -Direction Inbound -Action Allow -Protocol TCP -LocalPort 3389 -Profile Domain,Private -RemoteAddress 10.3.3.0/255.255.255.0,10.1.165.0/255.255.255.0,10.6.0.0/255.255.0.0`
- `New-NetFirewallRule -DisplayName "Escritorio remoto - Modo usuario (UDP de entrada)" -Direction Inbound -Action Allow -Protocol UDP -LocalPort 3389 -Profile Domain,Private -RemoteAddress`



10.3.3.0/255.255.255.0,10.1.165.0/255.255.255.0,10.6.0.0/255.255.0.

## **Configuración de backups en Proxmox**

Proxmox permite realizar backups de VMs en forma manual o automatizada. Las tareas de backups pueden realizarse íntegramente mediante la interfaz web de administración del clúster, aunque también es posible utilizar la consola de comandos para ello.

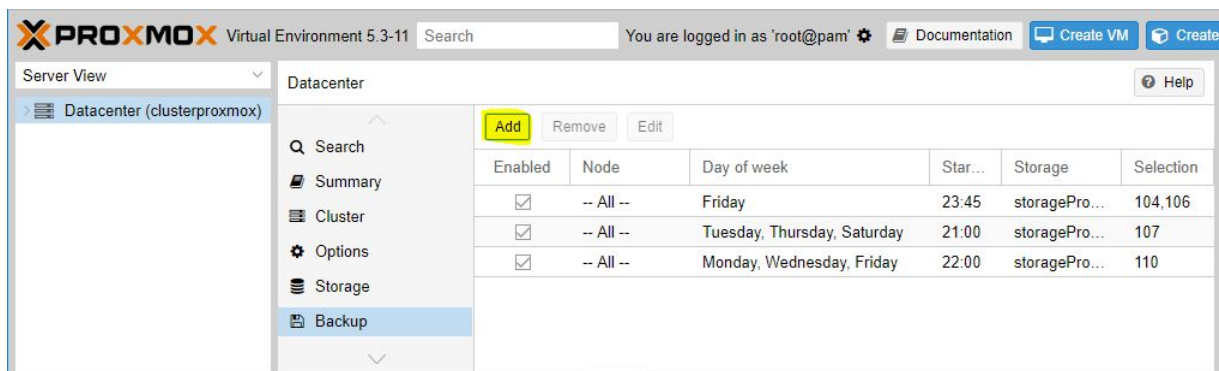
Antes de que se pueda ejecutar una copia de seguridad, se debe definir un almacenamiento de copia de seguridad. Un almacenamiento de copia de seguridad debe ser un almacenamiento de nivel de archivo, ya que las copias de seguridad se almacenan como archivos normales. En la mayoría de las situaciones, usar un servidor NFS es una buena manera de almacenar copias de seguridad.

Las tareas de copia de seguridad se pueden programar para que se ejecuten automáticamente en días y horas específicos, para nodos seleccionables y VMs. La configuración de las copias de seguridad programadas se realiza en el nivel de Datacenter en la GUI, lo que genera una entrada cron en `/etc/cron.d/vzdump`.

La restauración de una o más copias de seguridad grandes puede requerir una gran cantidad de recursos, especialmente el ancho de banda del almacenamiento, tanto para leer desde el almacenamiento de copia de seguridad como para escribir en el almacenamiento de destino. Esto puede afectar negativamente a otras VMs ya que el acceso al storage puede congestionarse. La configuración global se almacena en `/etc/vzdump.conf`.

A continuación se muestra un ejemplo de una tarea de backup programada mediante GUI y consola de comandos:

Desde la sección Datecenter, buscar la opción Backup y clicar en Add.



Seleccionar el destino de los backups, los días de la semana en los que se realiza la tarea, hora de inicio y las VMs involucradas. Para finalizar clicar en Create.

### Edit: Backup Job

Node:	<input type="text" value="-- All --"/>	Send email to:	<input type="text" value="notificaciones@frsf.utn.edu"/>
Storage:	<input type="text" value="storageProxmox"/>	Email notification:	<input type="text" value="On failure only"/>
Day of week:	<input type="text" value="Friday"/>	Compression:	<input type="text" value="LZO (fast)"/>
Start Time:	<input type="text" value="23:45"/>	Mode:	<input type="text" value="Snapshot"/>
Selection mode:	<input type="text" value="Include selected VMs"/>	Enable:	<input checked="" type="checkbox"/>

<input type="checkbox"/>	ID ↑	Node	Status	Name	Type
<input type="checkbox"/>	100	Nodo1	running	RDSH1	qemu
<input type="checkbox"/>	102	Nodo2	stopped	RDSH2	qemu

[? Help](#)
Create

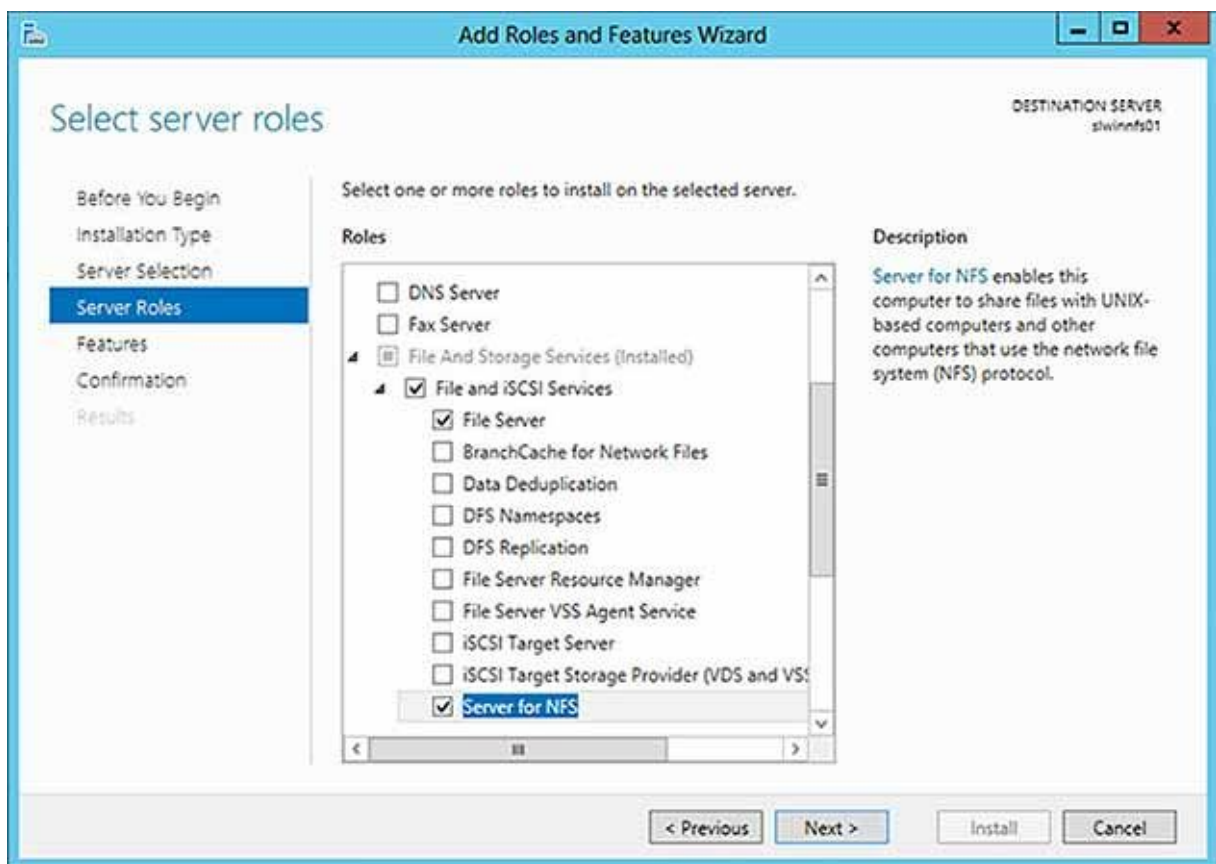
La creación de esta tarea genera un entrada en el archivo `/etc/cron.d/vzdump`.

```
45 23 * * 5 root vzdump 100 102 --mailnotification failure
--storage storageProxmox --quiet 1 --compress lzo --mailto
notificaciones@frsf.utn.edu.ar --mode snapshot
```

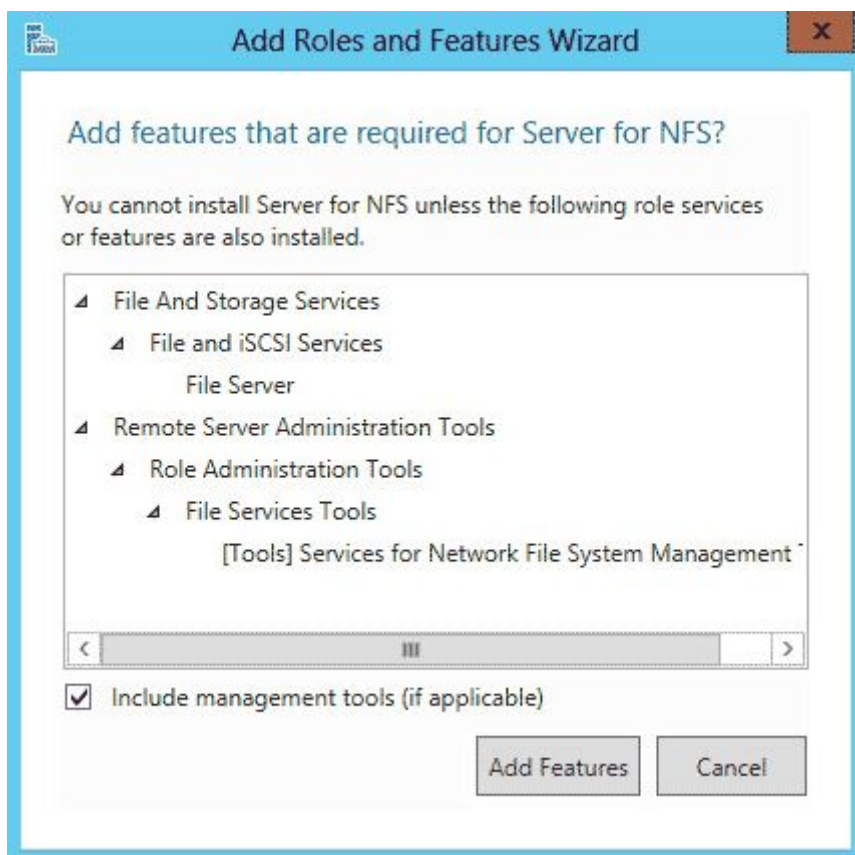
## Implementación de Rol de NFS en Windows Server

1. Iniciar el Administrador del Servidor.
2. En el menú superior, clicar en **Administrar**.

3. Clickear en **Agregar roles y características**.
4. En la pantalla Antes de comenzar, clickear en **Siguiente**.
5. En la pantalla Seleccionar tipo de instalación, asegurarse de que la **Instalación basada en roles o basada en funciones** esté seleccionada y luego clickear en **Siguiente**.
6. En la pantalla de selección de Servidor, clickear en **Siguiente**.
7. En la pantalla Seleccionar roles de servidor, expandir Servicios de archivo y almacenamiento, expandir Servicios de archivo e iSCSI y luego marcar **Servidor para NFS**.



8. Clickear en **Siguiente**.
9. Si aparece un cuadro de diálogo Agregar características que son necesarias para Servidor NFS, clickear en **Agregar características**.

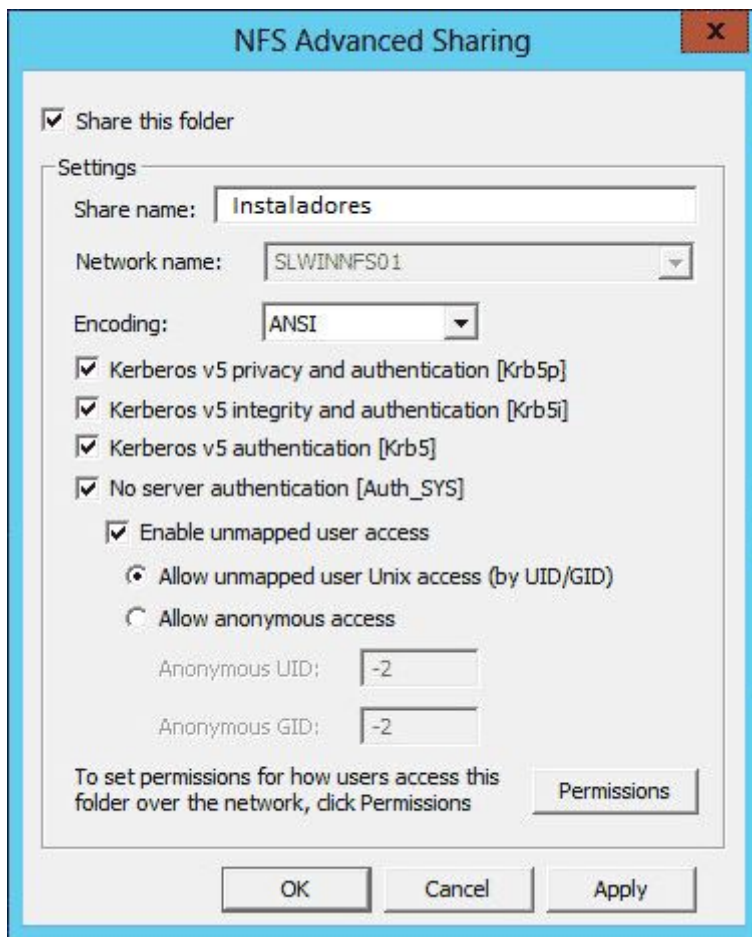


10. En la pantalla Seleccionar función, clicar en **Siguiente**.

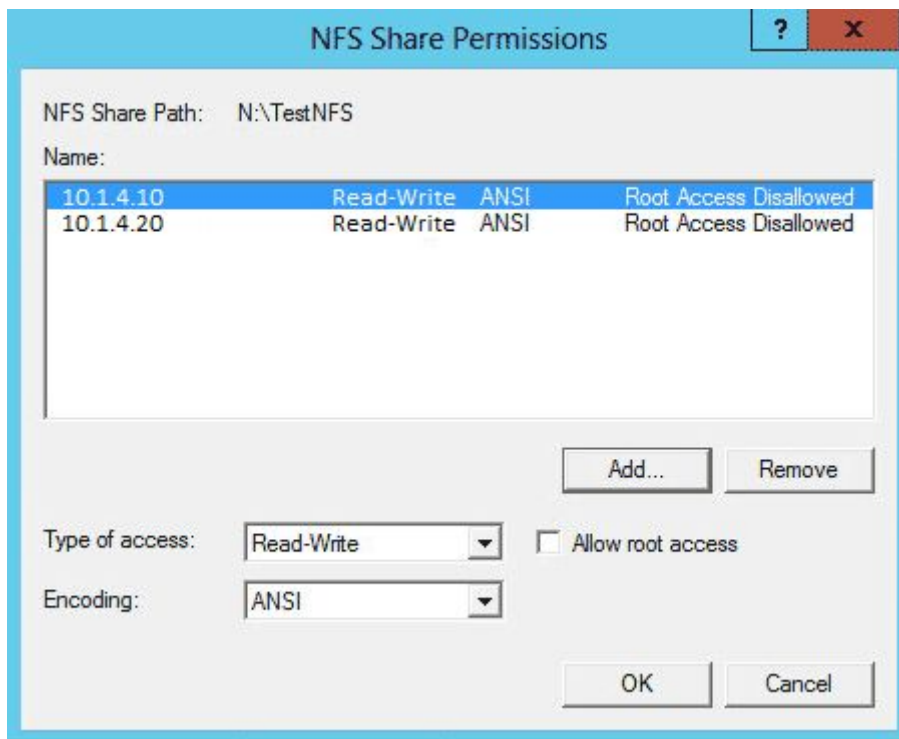
11. Confirmar los detalles de la instalación y luego clicar en **Instalar**.

### **Configurar un recurso compartido NFS**

1. Iniciar el Explorador de archivos.
2. Crear un nuevo directorio para el NFS compartido.
3. Clicar con botón derecho en el directorio y clicar en **Propiedades**.
4. Seleccionar la pestaña **Compartir NFS**.
5. En la pestaña Compartir NFS, clicar en el botón **Administrar uso compartido de NFS**.
6. Marcar la casilla de verificación **Compartir esta carpeta**.



7. Introducir un nombre en el campo de texto Compartir nombre. Esto se utilizará cuando un usuario se conecte al recurso compartido NFS.
8. Clickear en el botón **Permisos**.
9. Clickear en **Agregar** y luego ingresar la dirección IP o el nombre de host de los clientes a los que desea permitir las conexiones. Cuando se agrega, también puede seleccionar si tienen acceso de escritura o acceso de solo lectura.



10. Clickear en **Aceptar**.

11. Clickear en **Aplicar** y luego en **Aceptar**.

## Gráficas de la primer etapa de pruebas

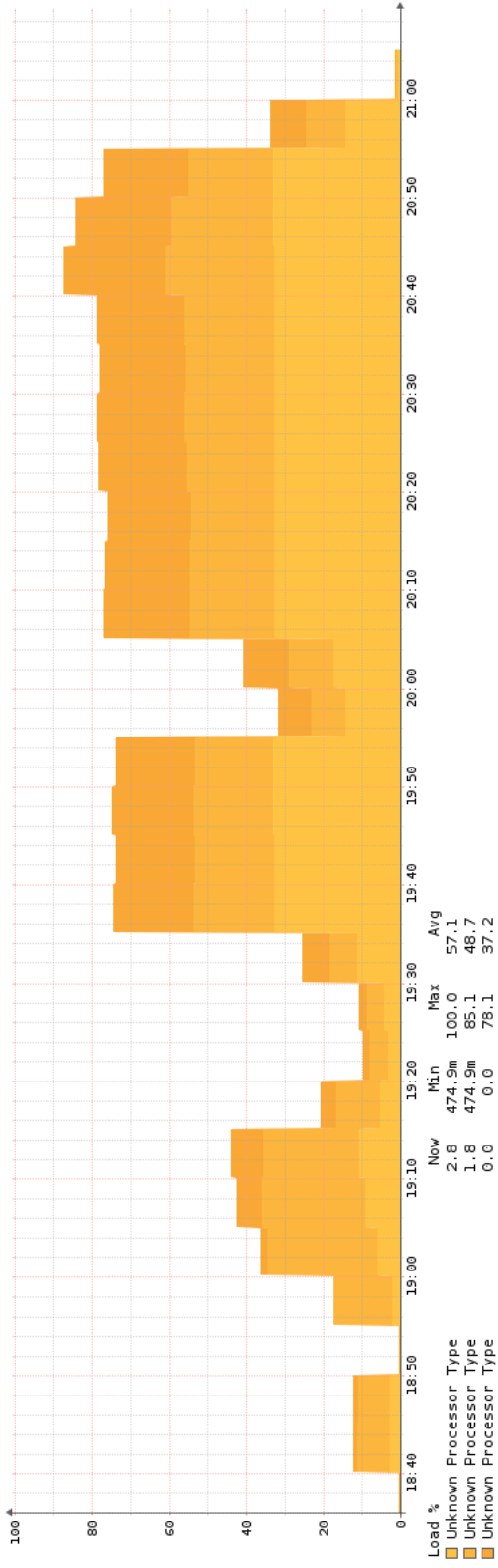
A continuación se presentan las gráficas de los indicadores monitoreados sobre los dispositivos utilizados en las pruebas de la sección 4.6.

### Pruebas sobre el software Simio 6

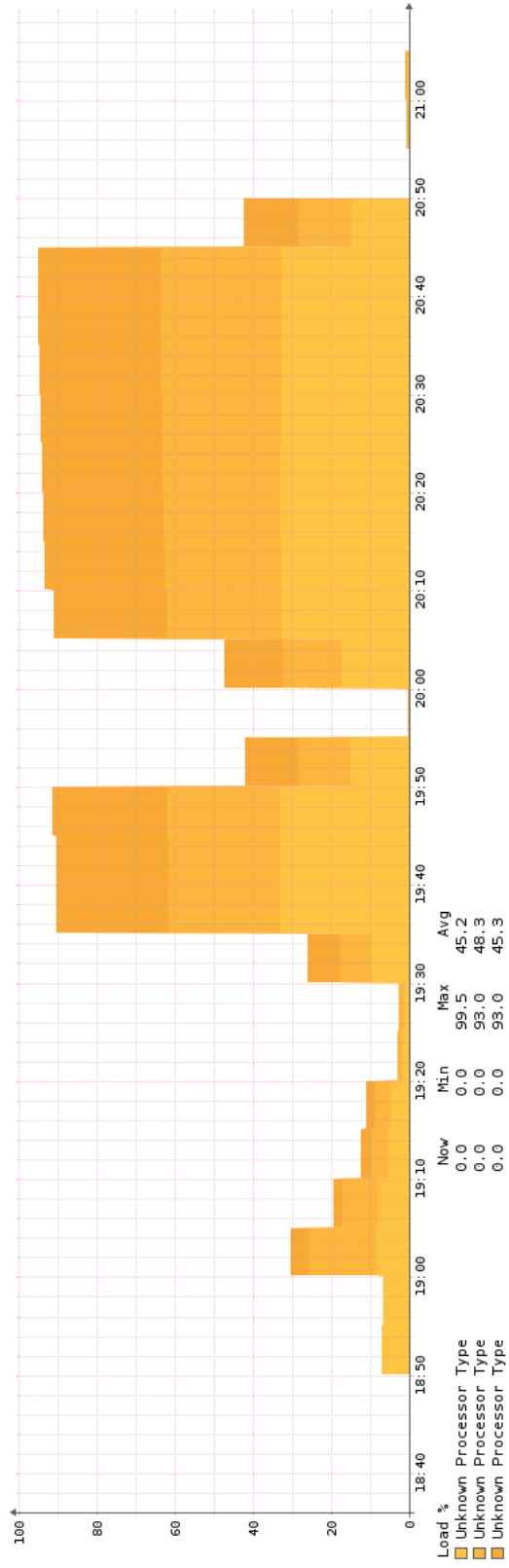
Se monitoreó el uso de procesador, memoria ram y red en los servidores RDSH1 y RDSH1, y el uso de red en el switch de acceso de las pcs cliente.

## Uso de procesador en servidores RDSH1 y RDSH2

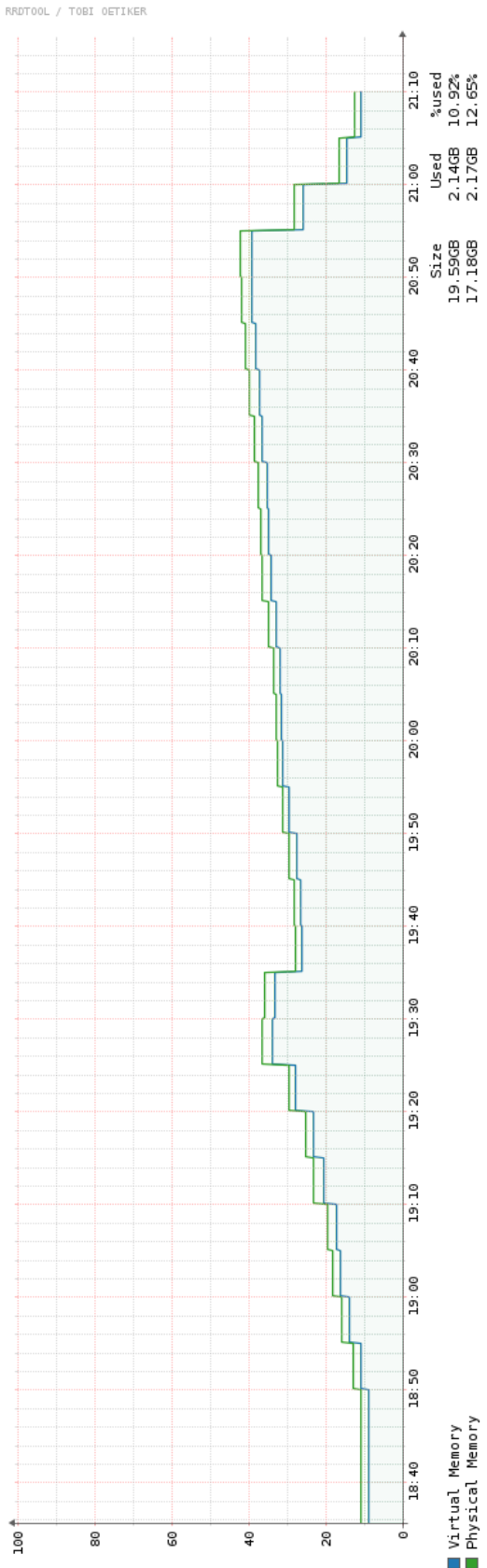
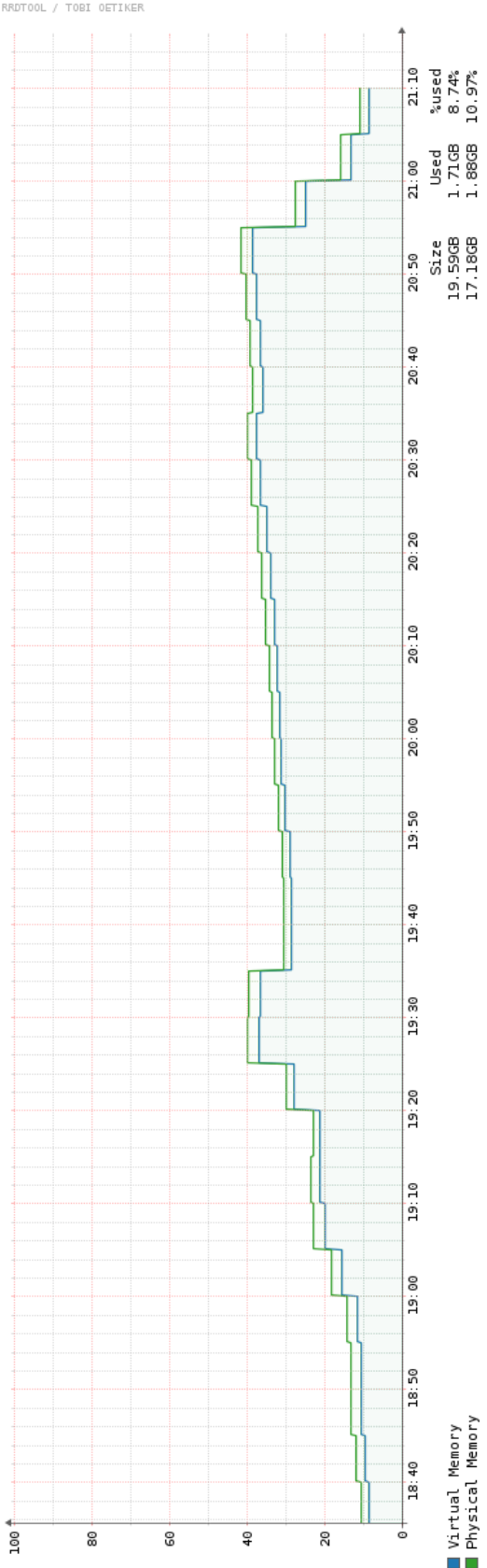
RRDTOOL / TOBI OETIKER



RRDTOOL / TOBI OETIKER

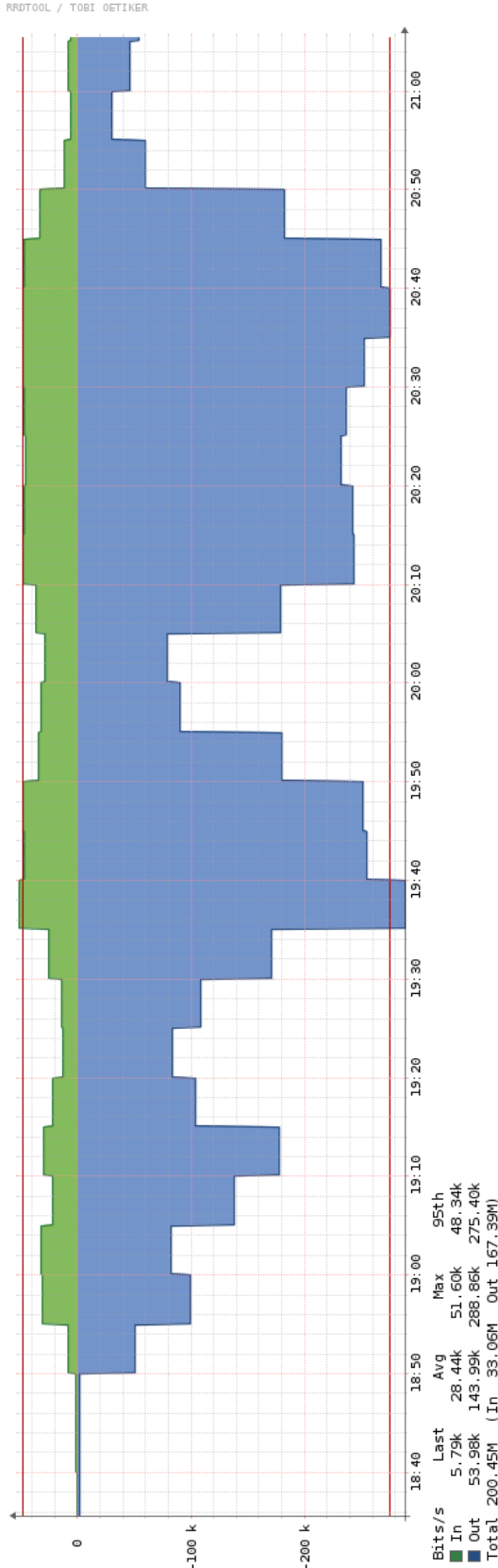
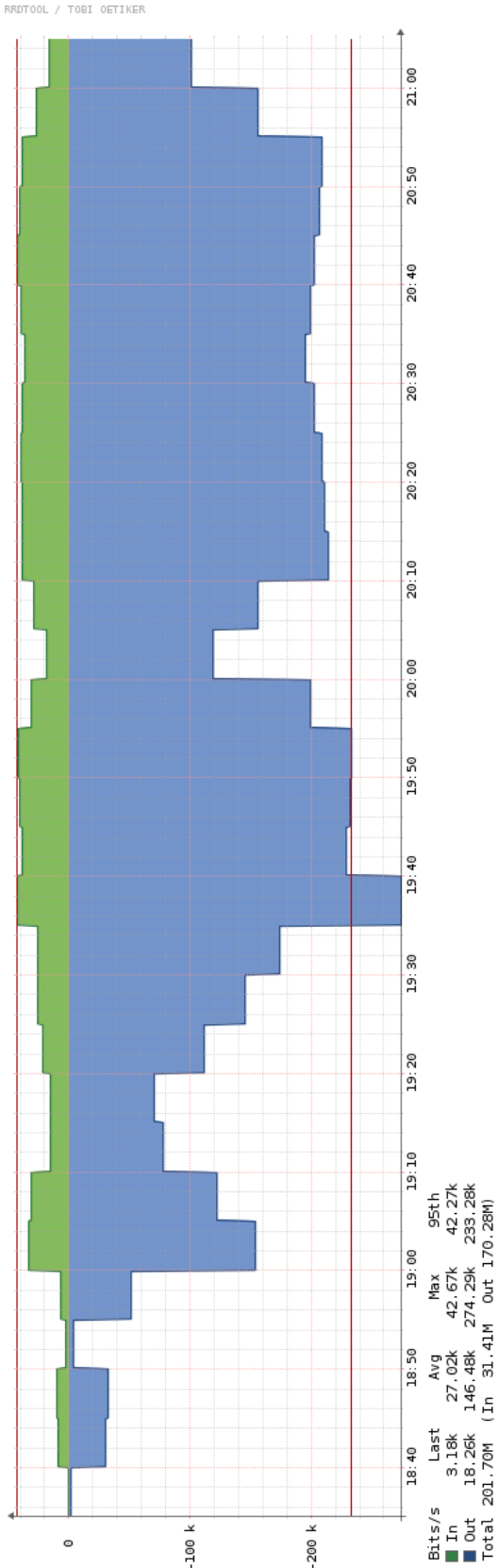


# Uso de memoria en servidores RDSH1 y RDSH2

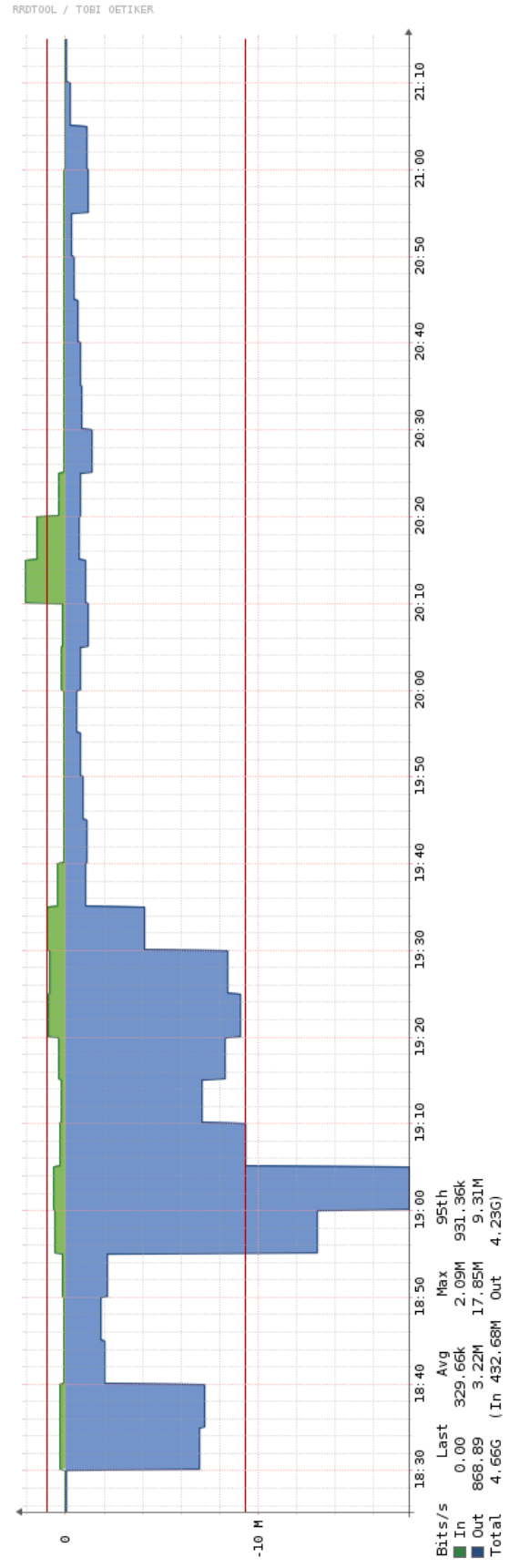




# Uso de red en RDSH1 y RDSH2



# Uso de red en switch de acceso

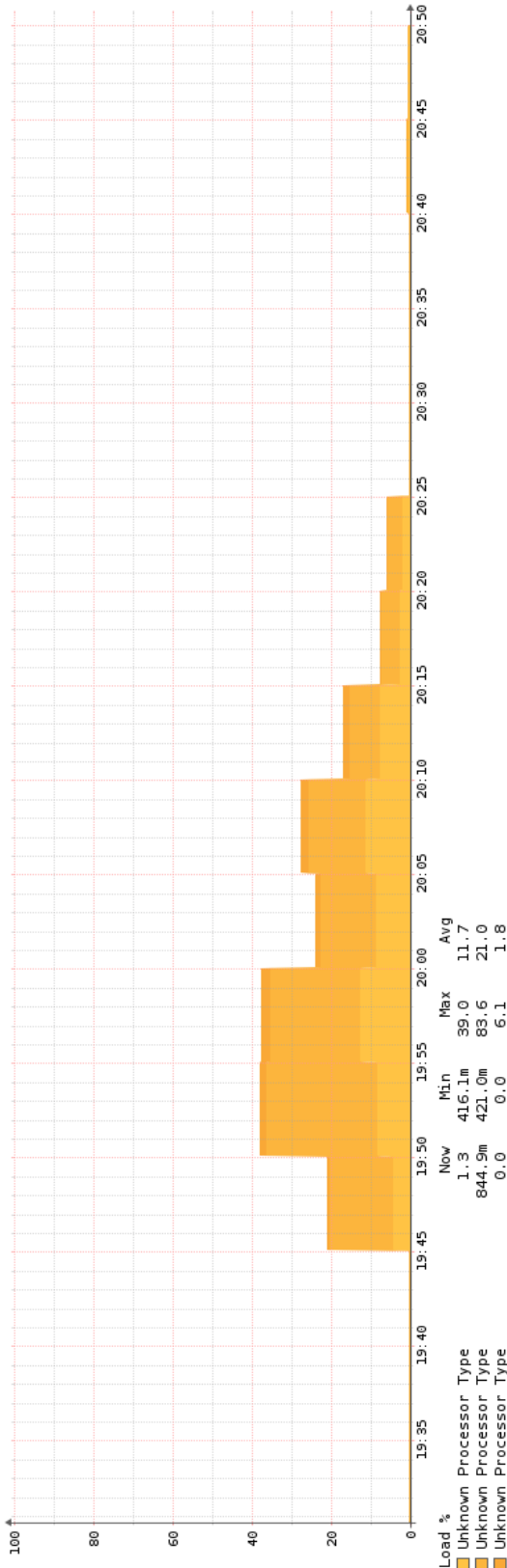


## **Pruebas sobre el software Autocad 2018**

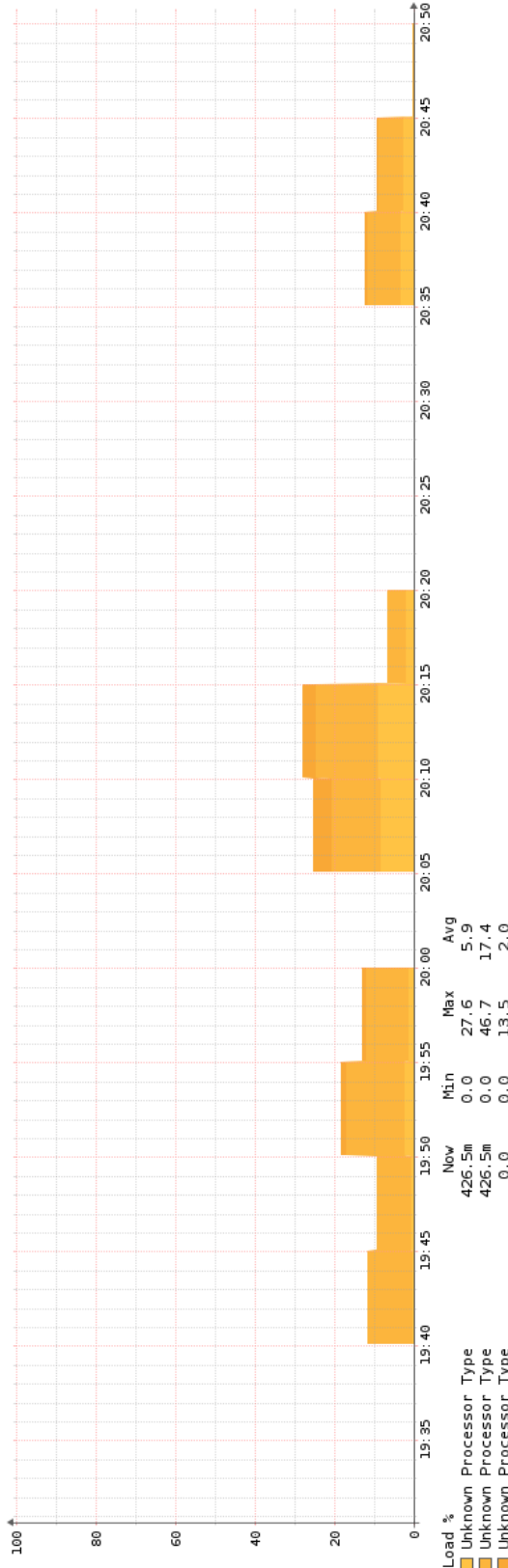
Se monitoreó el uso de procesador, memoria y red en los servidores RDSH1 y RDSH2, y el uso de red en el switch de acceso de las pcs cliente.

# Uso de procesador en servidores RDSH1 y RDSH2

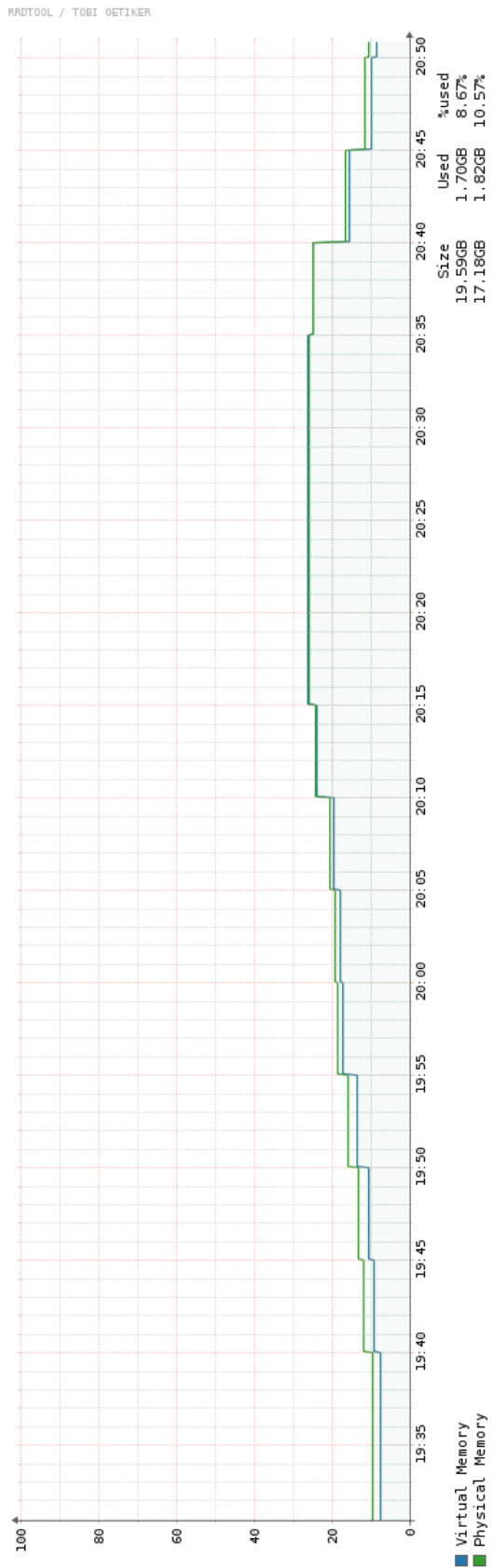
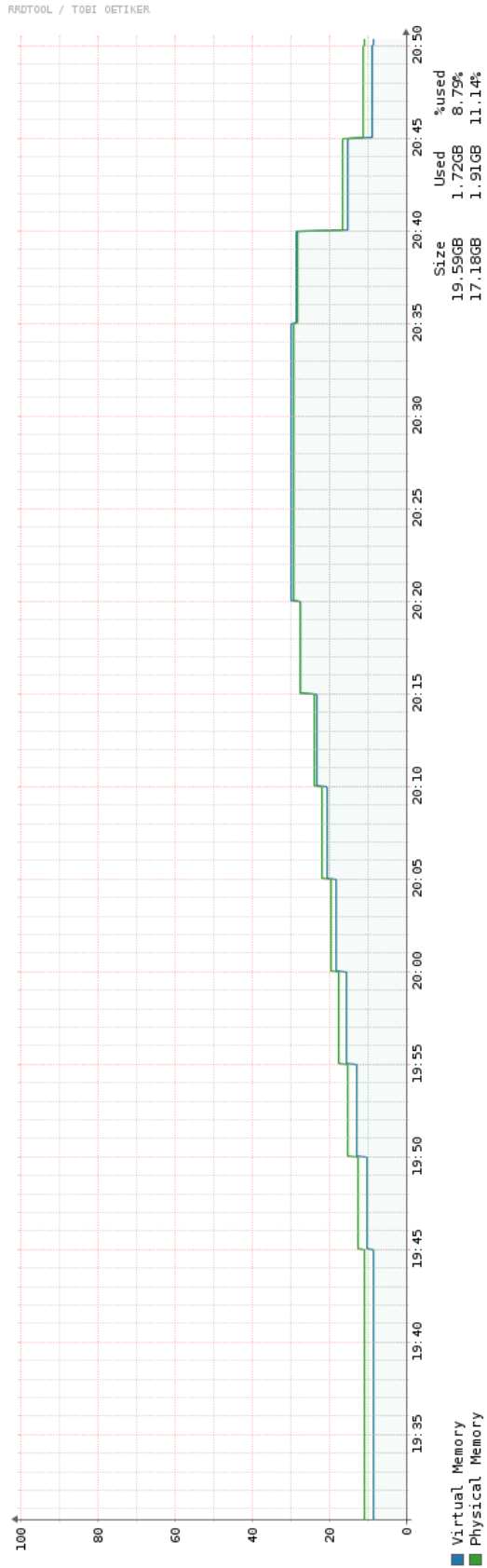
RRDTOOL / TOBI OETIKER



RRDTOOL / TOBI OETIKER

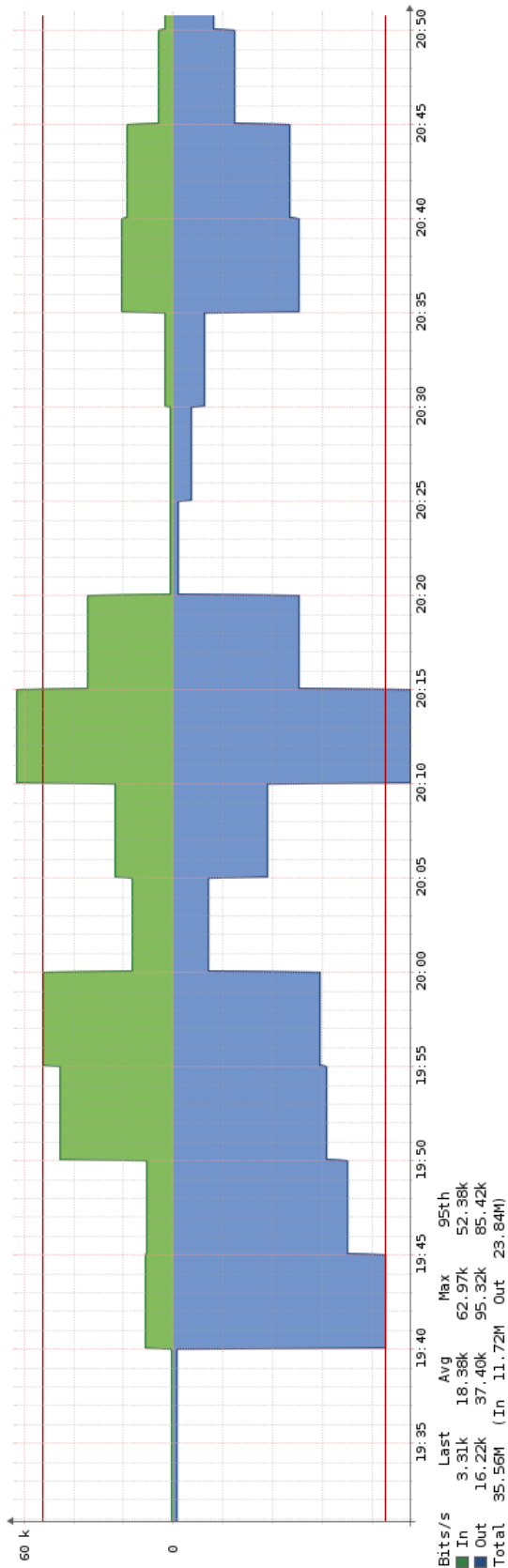


## Uso de memoria en servidores RDSH1 y RDSH2

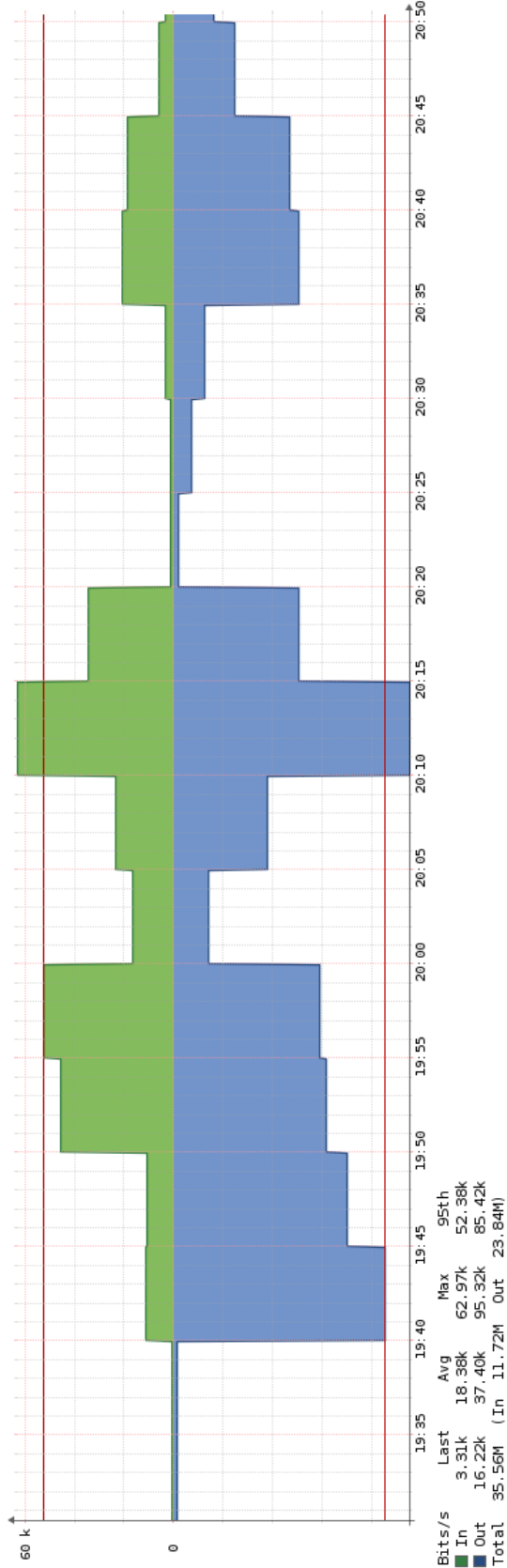


# Uso de red en servidores RDSH1 y RDSH2

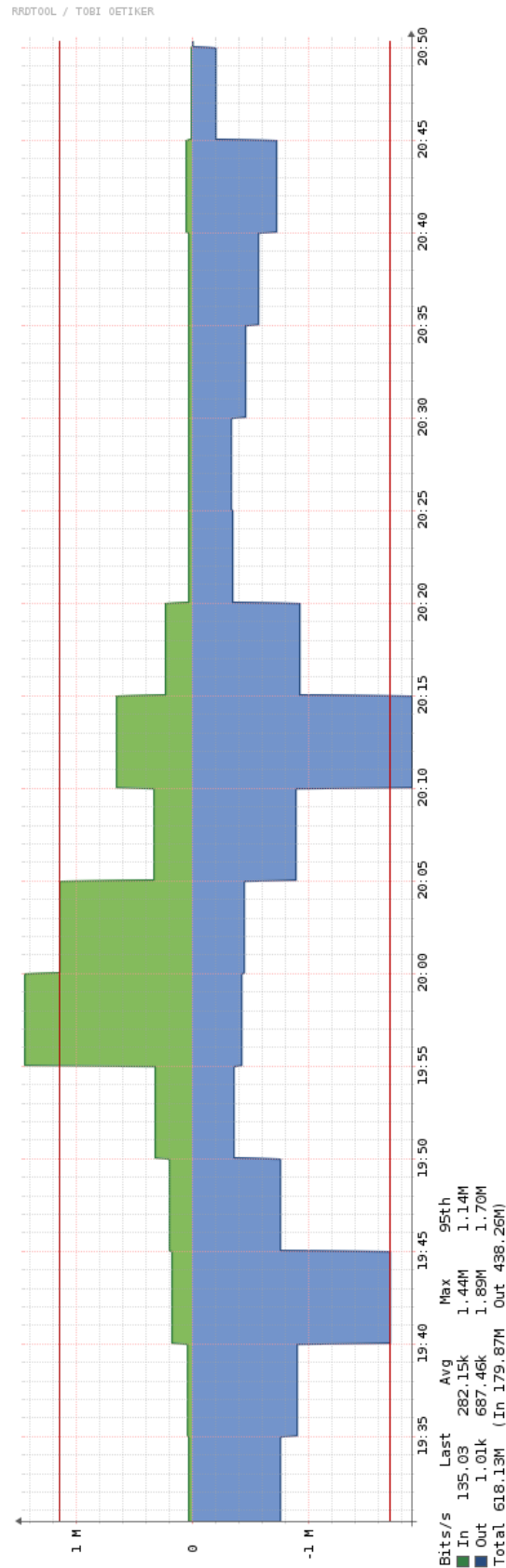
RRDTOOL / TOBI OETIKER



RRDTOOL / TOBI OETIKER



# Uso de red en switch de acceso



## Configuraciones de red Wifi

La red wifi utilizada para la aplicación de campo está basada en APs autónomos con controlador central de la marca Ubiquiti. Los detalles de la implementación del controlador exceden el alcance de este informe, por lo que sólo presentamos la configuración de la WLAN necesaria para la aplicación y la configuración de los switch de acceso al AP.

Accedemos al controlador por web, seleccionamos el AP a utilizar y en el apartado WLANS seleccionamos la red a utilizar y dentro de la configuración de la red definimos: VLAN de la red de clientes (165), el nombre del SSID de la red wifi y la contraseña de acceso.

The screenshot displays the configuration page for a WLAN on a Ubiquiti controller. The top section shows the AP name 'WLabMovil2' with a 'DISCONNECTED' status. Below this, a signal strength indicator shows '11 11N/B/G (Good)' and '6% Utilized'. A legend indicates the status of RX FRAMES, TX FRAMES, INTERFERENCE, and FREE. The 'Config' tab is selected, and the 'WLAN 2G (11N/B/G) - OVERRIDE DEPARTAMENTAL1 WIFIO' configuration is shown. The configuration includes a checked box for 'Enabled on this AP', a checked box for 'Use VLAN with VLAN ID 165', an SSID field containing 'labmovil', and a Security Key field with masked characters. At the bottom, there are buttons for 'SAVE', 'RESET TO DEFAULTS', and 'CANCEL'.



De este modo, el AP publicará un SSID de nombre “labmovil” con acceso a la red en la vlan 165. Adicionalmente, el puerto del switch donde se conecte el AP debe configurarse en modo troncal, con las vlan 1 sin etiquetar (utilizada para la red de administración de los AP) y la vlan 165 etiquetada (para dar servicio de red a los clientes inalámbricos). A continuación se muestra un ejemplo de configuración de un puerto de switch HP:

```
interface Ethernet1/0/24

  stp edged-port enable

  port link-type hybrid

  port hybrid vlan 165 tagged

  port hybrid vlan 1 untagged

#
```

## **Listas de Control de Acceso**

### **Pautas generales para la creación de una ACL**

La composición de ACL puede ser una tarea compleja. Para cada interfaz, puede haber varias políticas necesarias para administrar el tipo de tráfico que tiene permitido ingresar a la interfaz o salir de ella.

Las siguientes son algunas pautas para el uso de ACL:

- Utilice las ACL en los routers de firewall ubicados entre su red interna y una red externa, como Internet.
- Utilice las ACL en un router ubicado entre dos partes de la red para controlar el tráfico que entra a una parte específica de su red interna o que sale de esta.
- Configure las ACL en los routers de frontera, es decir, los routers ubicados en los límites de las redes. Esto proporciona una separación muy básica de la red externa o entre un área menos controlada y un área más importante de su propia red.

- Configure las ACL para cada protocolo de red configurado en las interfaces del router de frontera.

Para recordar una regla general de aplicación de ACL en un router, puede pensar en “las tres P”. Se puede configurar una ACL por protocolo, por sentido y por interfaz:

- Una ACL por protocolo: para controlar el flujo de tráfico en una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz.
- Una ACL por sentido: las ACL controlan el tráfico en una interfaz de a un sentido por vez. Se deben crear dos ACL diferentes para controlar el tráfico entrante y saliente.
- Una ACL por interfaz: las ACL controlan el tráfico para una interfaz.

### **Dónde ubicar las ACL**

La correcta colocación de las ACL puede contribuir a que la red funcione de forma más eficaz. Se puede colocar una ACL para reducir el tráfico innecesario. Por ejemplo, el tráfico que se denegará en un destino remoto no se debe reenviar mediante recursos de red por la ruta hacia ese destino.

Cada ACL se debe colocar donde tenga más impacto en la eficiencia. Las reglas básicas son las siguientes:

- ACL extendidas: coloque las ACL extendidas lo más cerca posible del origen del tráfico que se filtrará. De esta manera, el tráfico no deseado se deniega cerca de la red de origen, sin que cruce la infraestructura de red.
- ACL estándar: debido a que en las ACL estándar no se especifican las direcciones de destino, colóquelas tan cerca del destino como sea posible. Si coloca una ACL estándar en el origen del tráfico, evitará de forma eficaz que ese tráfico llegue a cualquier otra red a través de la interfaz a la que se aplica la ACL.

La colocación de la ACL y, por lo tanto, el tipo de ACL que se utiliza también puede depender de lo siguiente:

- Alcance del control del administrador de la red: la colocación de la ACL puede depender de si el administrador de red controla tanto la red de origen como la de destino o no.

- Ancho de banda de las redes involucradas: el filtrado del tráfico no deseado en el origen impide la transmisión de ese tráfico antes de que consuma ancho de banda en la ruta hacia un destino. Esto es de especial importancia en redes con un ancho de banda bajo.
- Facilidad de configuración: si un administrador de red desea denegar el tráfico proveniente de varias redes, una opción es utilizar una única ACL estándar en el router más cercano al destino. La desventaja es que el tráfico de dichas redes utilizará ancho de banda de manera innecesaria. Se puede utilizar una ACL extendida en cada router donde se origina tráfico. Esto ahorra ancho de banda, ya que el tráfico se filtra en el origen, pero requiere la creación de ACL extendidas en varios routers.

### **Gráficas de la segunda etapa de pruebas**

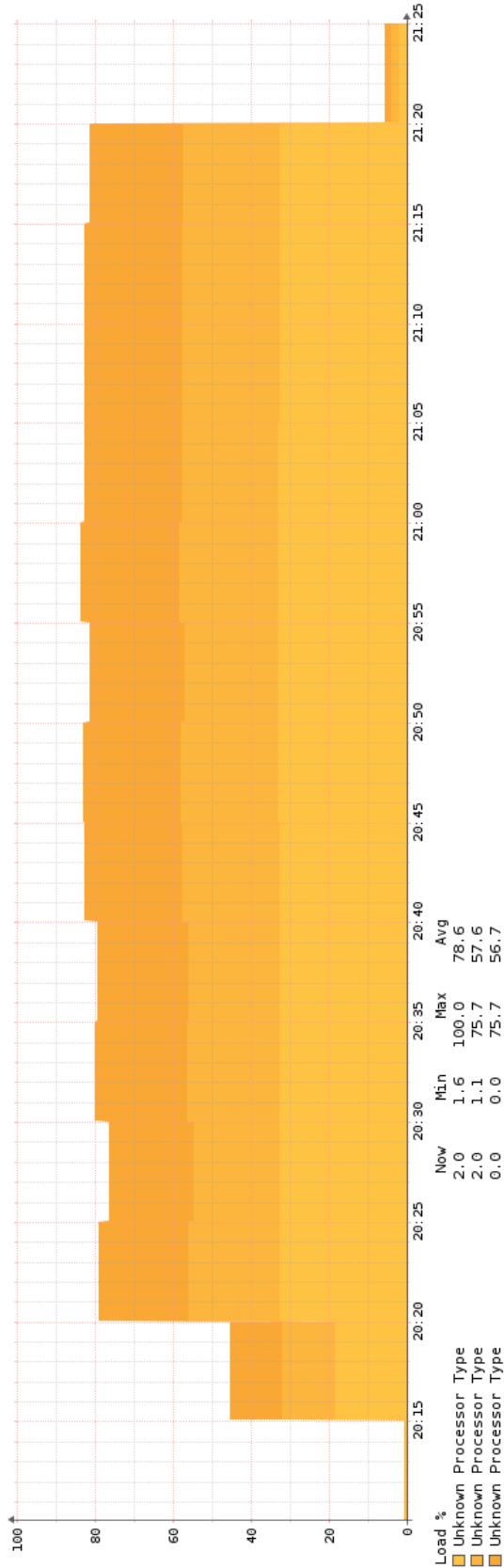
A continuación se presentan las gráficas de los indicadores monitoreados sobre los dispositivos utilizados en las pruebas de la sección 5.5.

#### **Pruebas sobre el software Simio 6**

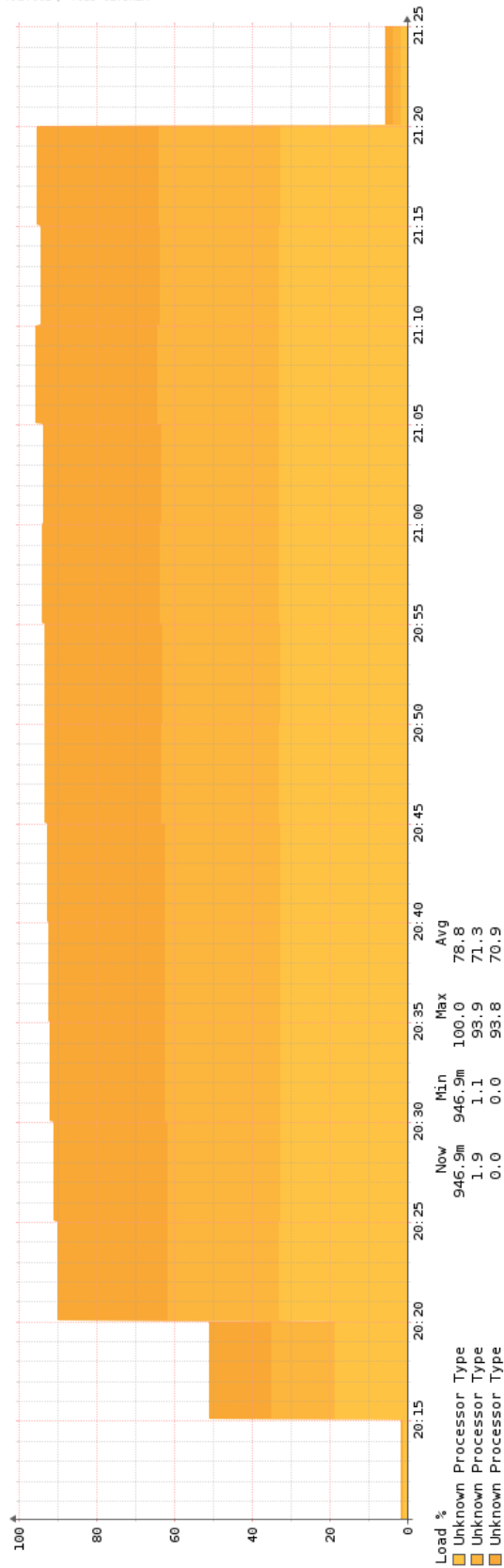
Se monitoreó el uso de procesador, memoria y red en los servidores RDSH1, RDSH2 y del Access Point de la red wifi.

# Uso de procesador en servidores RDSH1 y RDSH2

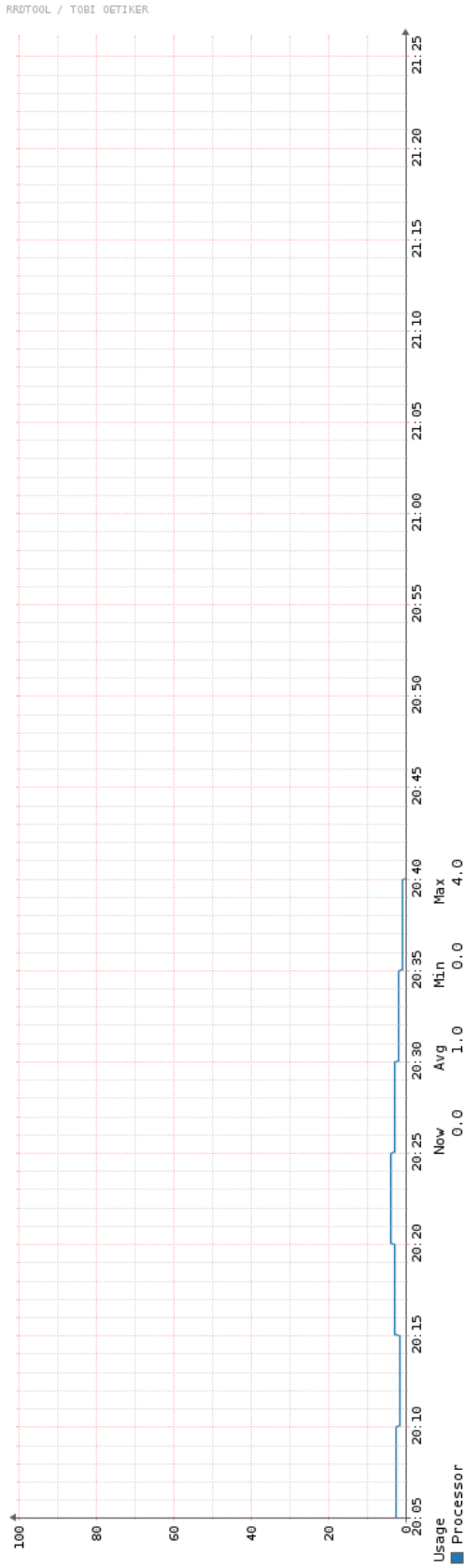
RRDTOOL / TOBI OETIKER



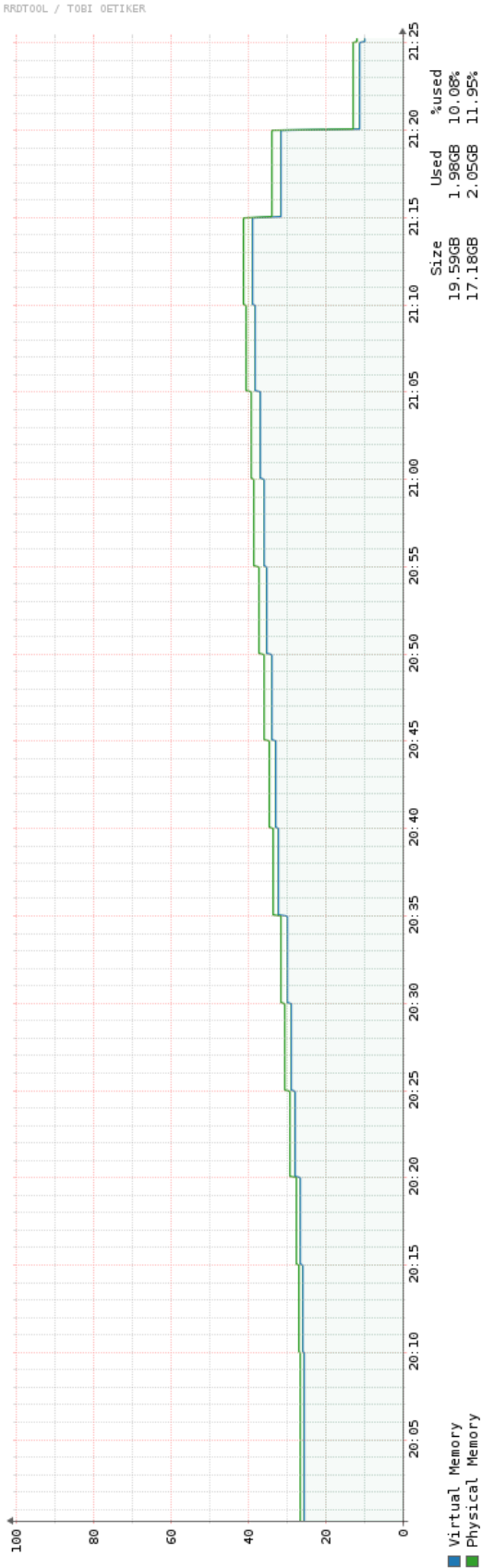
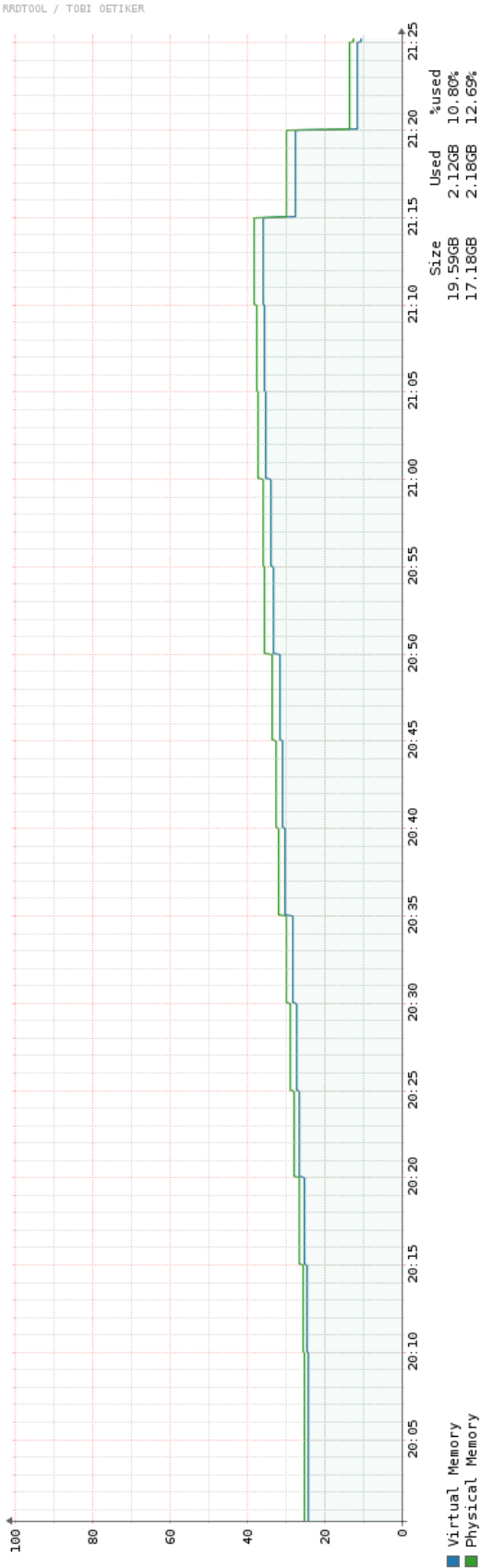
RRDTOOL / TOBI OETIKER



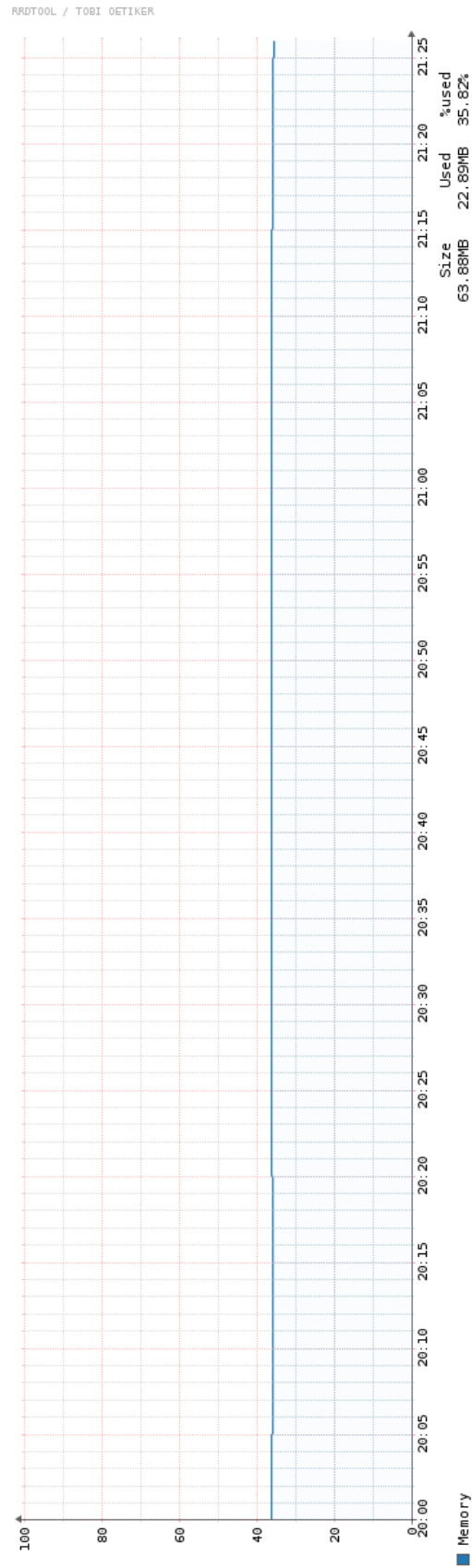
# Uso de procesador en Access Point



# Uso de memoria en servidores RDSH1 y RDSH2

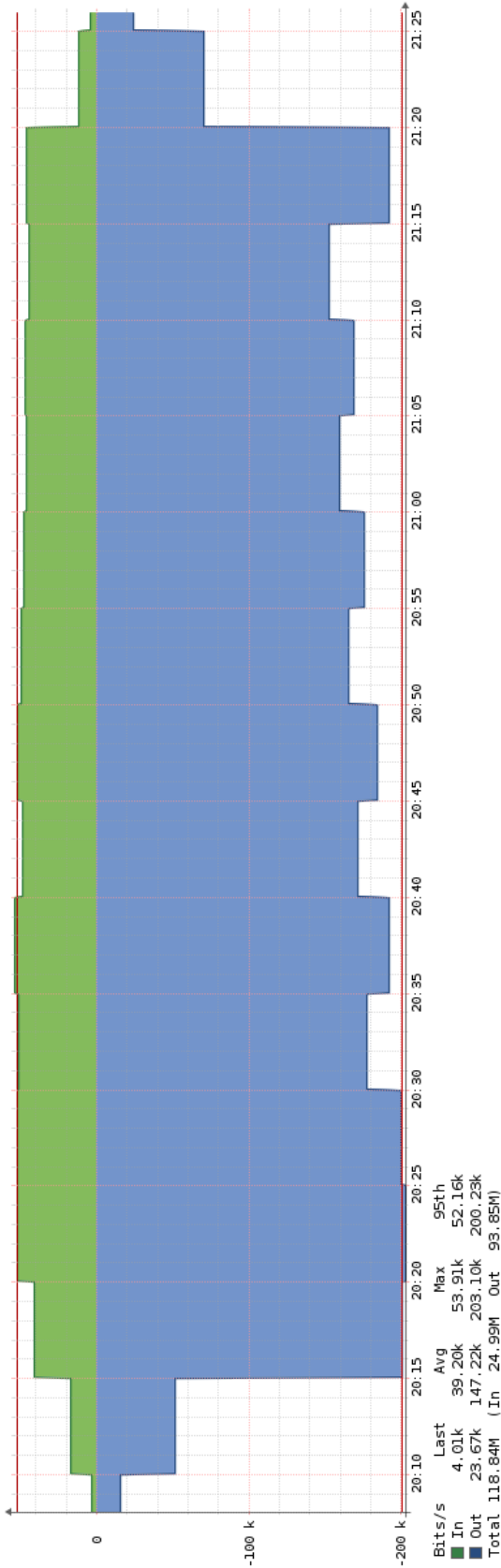


# Uso de memoria en Access Point

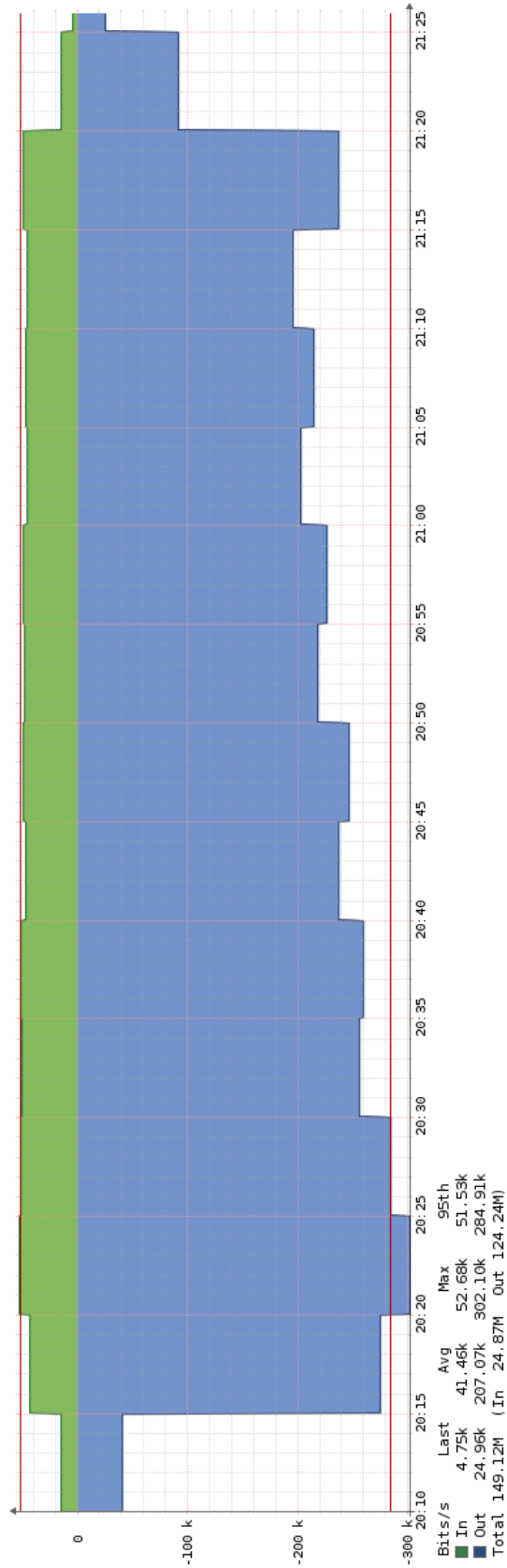


## Uso de red en servidores RDSH1 y RDSH2

RRDTOOL / TOBI OETIKER



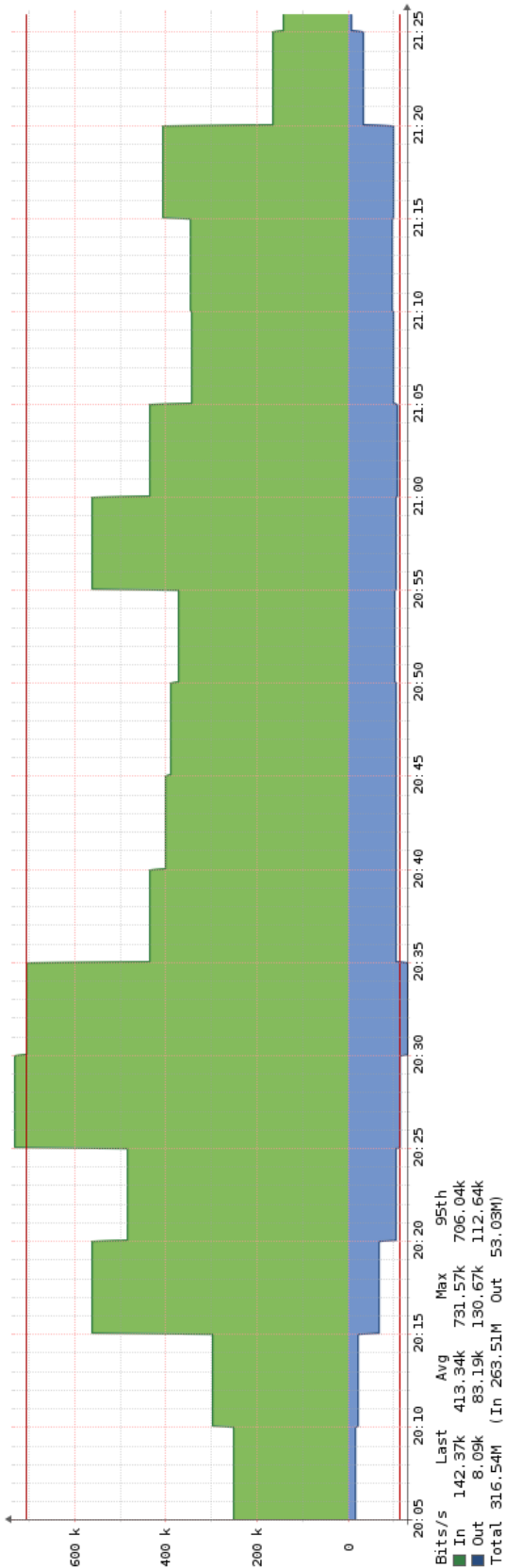
RRDTOOL / TOBI OETIKER





# Uso de red en Access Point

RRDTOOL / TOBI OETIKER

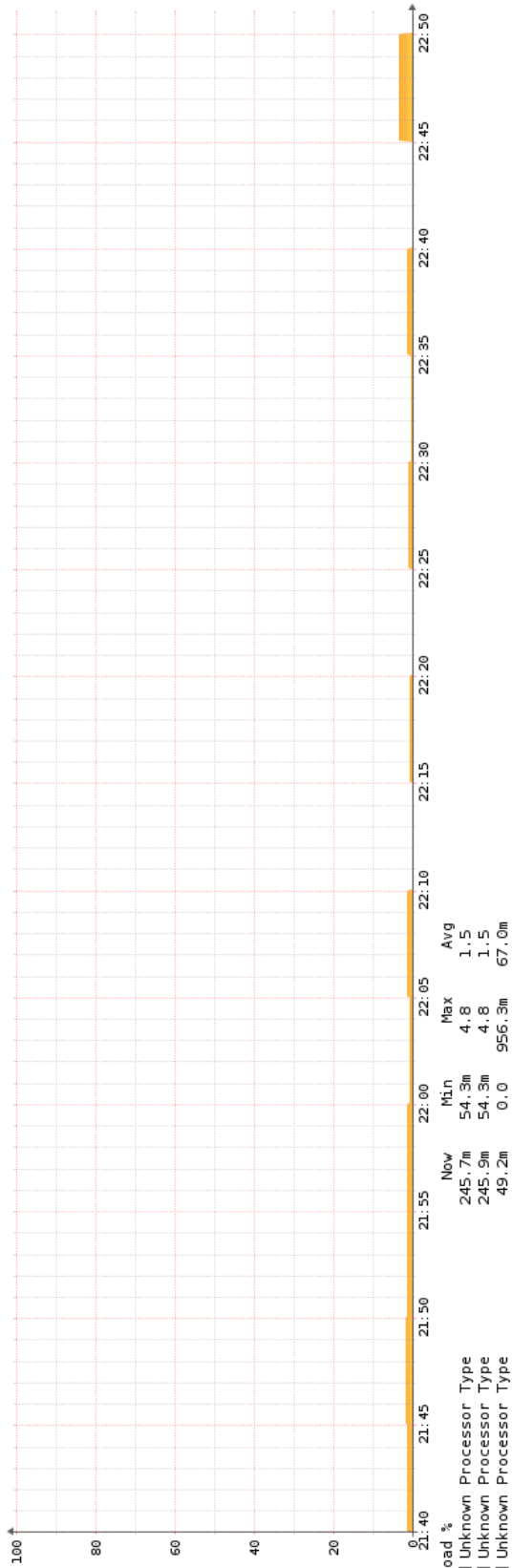


## **Pruebas sobre el software Autocad 2018**

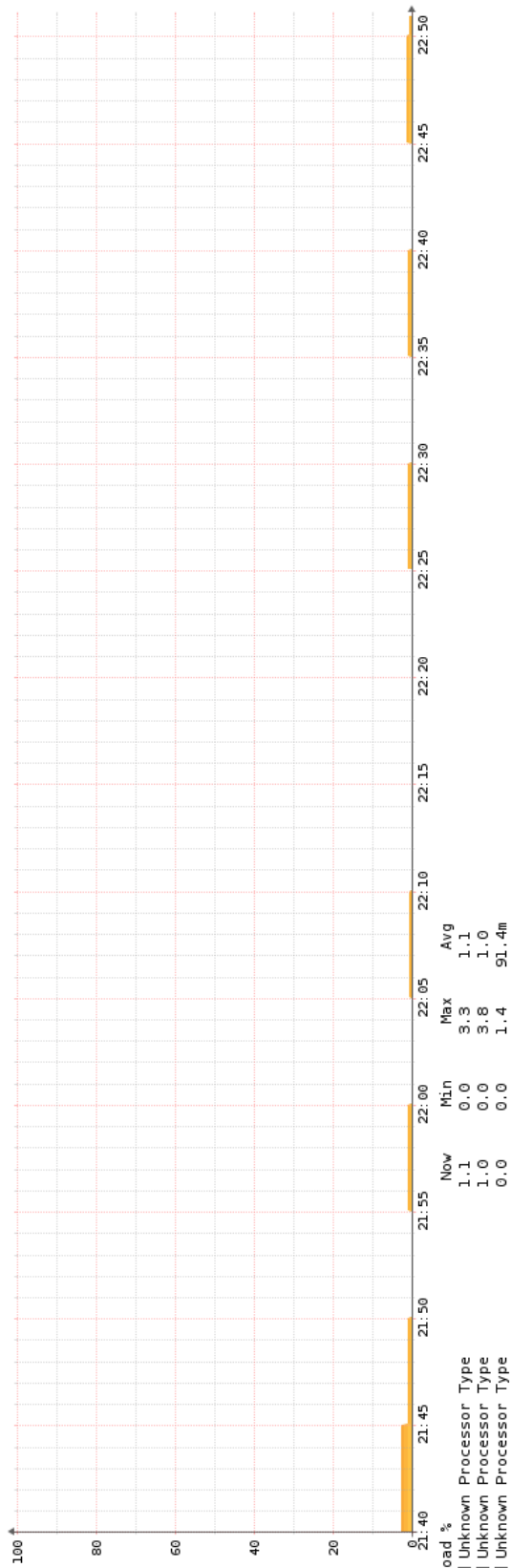
Se monitoreó el uso de procesador, memoria y red en los servidores RDSH1, RDSH1 y del Access Point de la red wifi.

# Uso de procesador en servidores RDSH1 y RDSH2

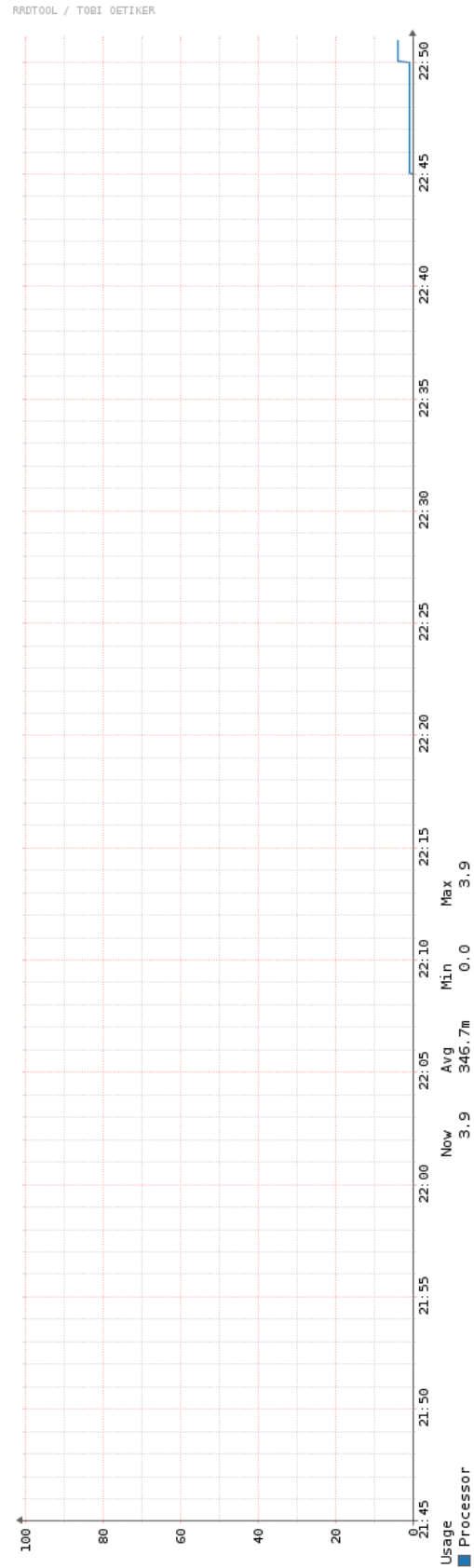
RRDT00L / T0BI 0ETIKER



RRDT00L / T0BI 0ETIKER

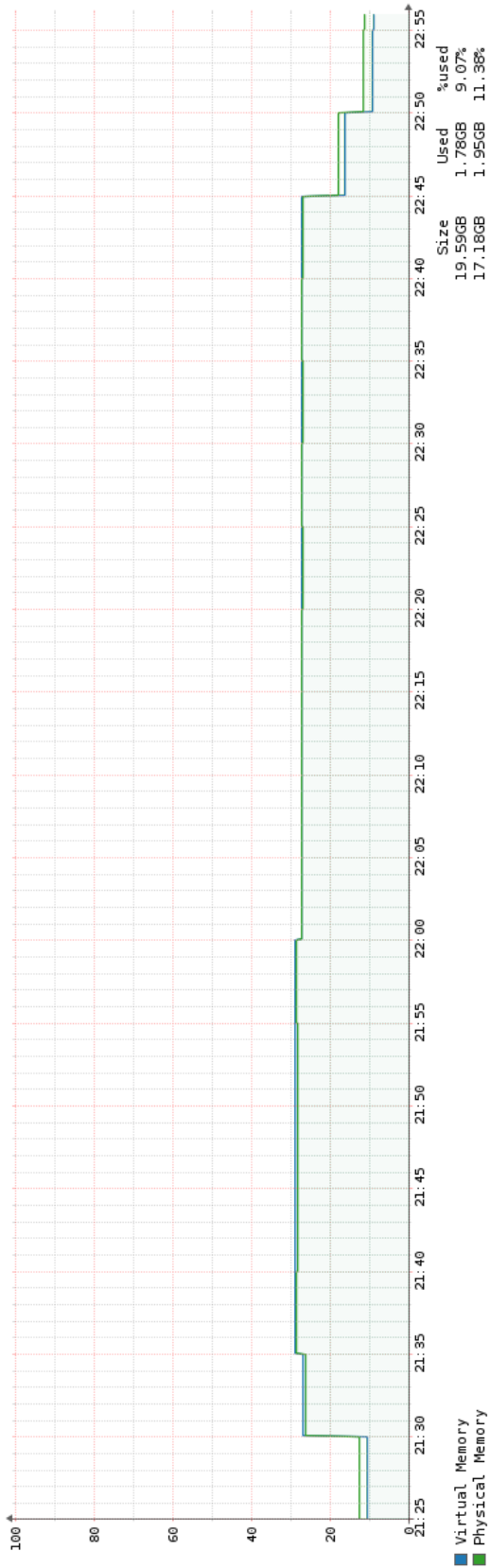


# Uso de procesador en Acess Point

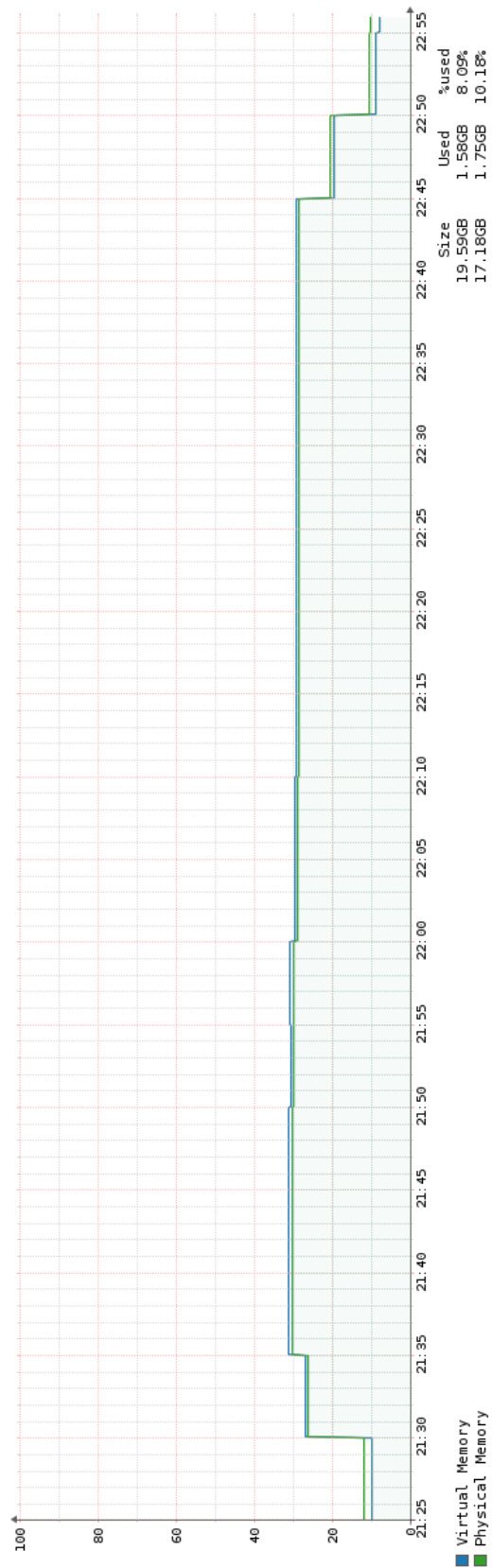


## Uso de memoria en servidores RDSH1 y RDSH2

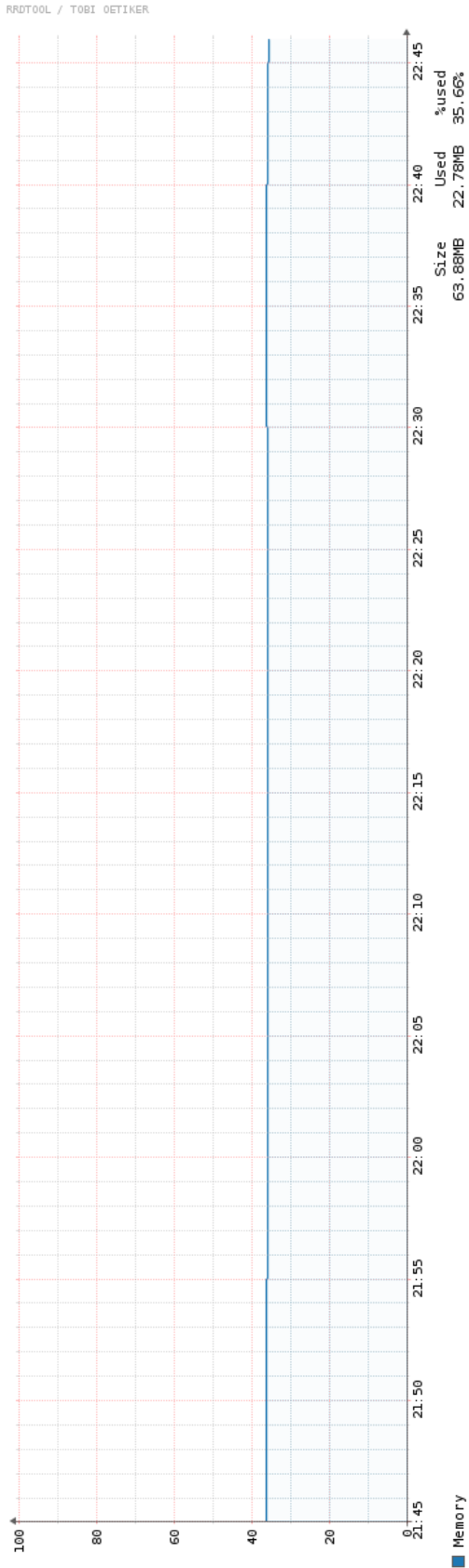
RRDTOOL / TOBI OETIKER



RRDTOOL / TOBI OETIKER

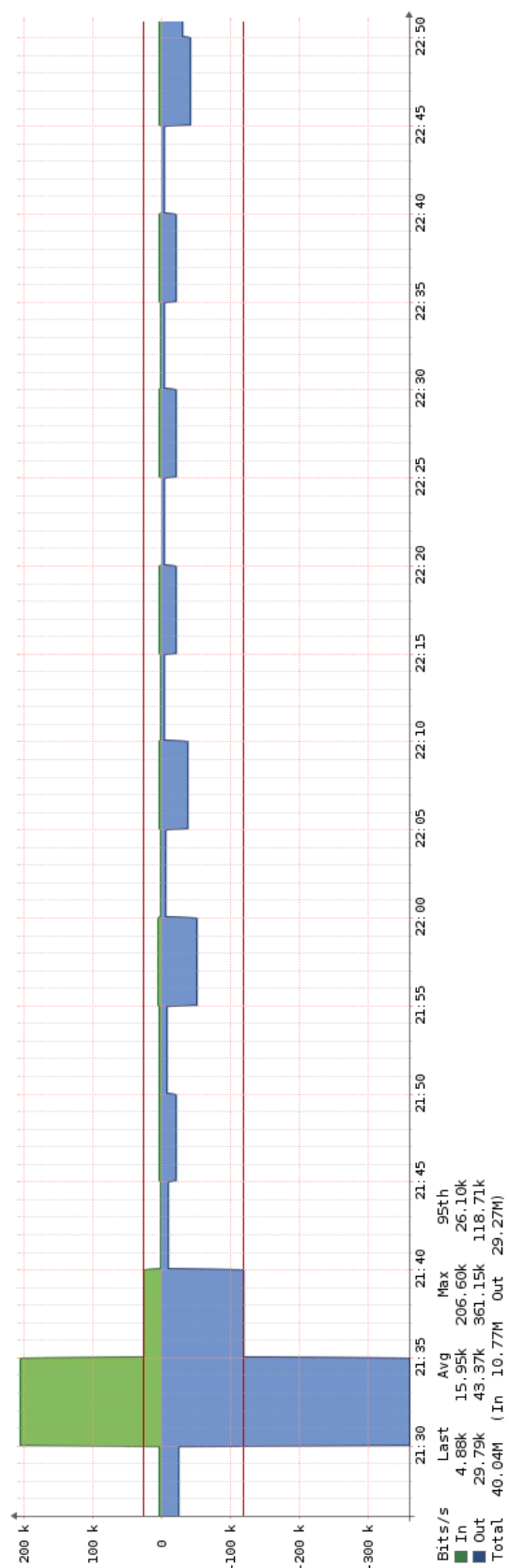


# Uso de memoria en Access Point

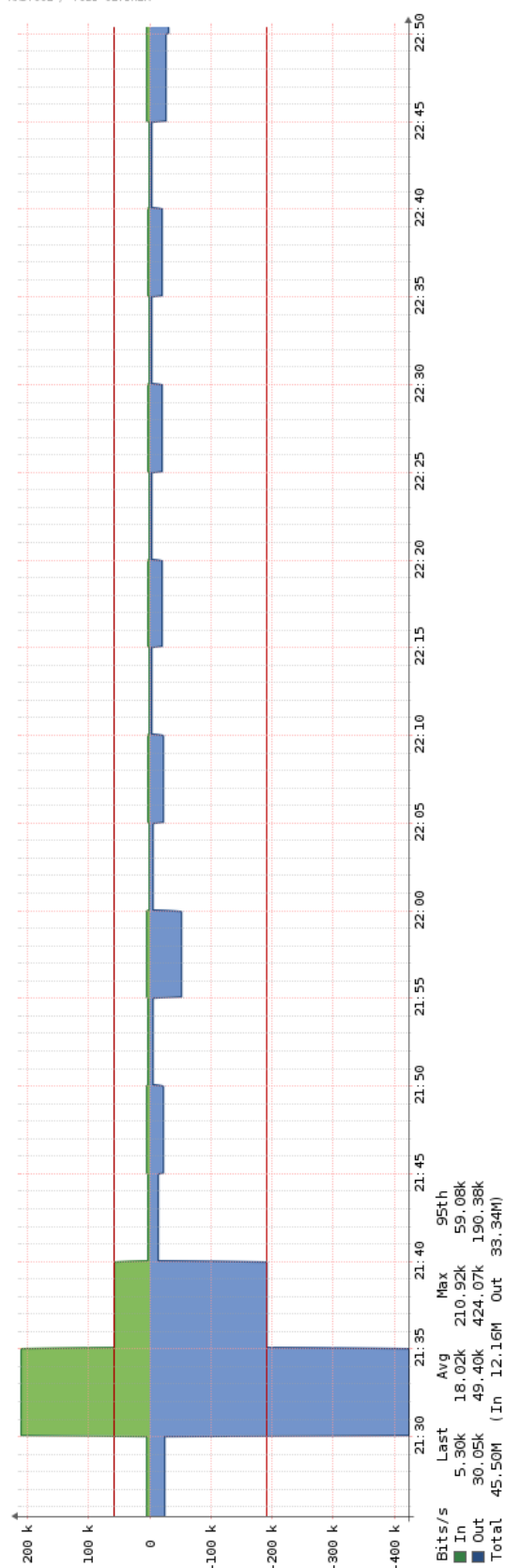


## Uso de red en servidores RDSH1 y RDSH2

RRDTOOL / TOBI OETIKER



RRDTOOL / TOBI OETIKER



# Uso de red en Access Point

RADTOOL / TOBI OETIKER

