

Servidores web de altas prestaciones en entornos virtualizados

Ángel Gómez Martín
agomezm@correo.ugr.es
SWAP - ETSIIT 2017-18

Virtualización

- Es 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.
- Se refiere a la abstracción de los recursos de una máquina, llamada hypervisor o VMM (Virtual Machine Monitor) que crea una capa de abstracción entre el hardware de la máquina física (host) y el SO de la VM (virtual machine, guest), dividiéndose el recurso en uno o más entornos de ejecución.

Hypervisor

- Un **hipervisor** una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en una misma máquina. Presentan a los sistemas operativos virtualizados una plataforma operativa virtual, a la vez que ocultan a dicho sistema operativo virtualizado las características físicas reales del equipo sobre el que operan.

Tipos de hipervisores

- Tipo 1



- Tipo 2



Ventajas

- **Seguridad:** cada máquina tiene un acceso privilegiado independiente.
- **Aislamiento:** las máquinas virtuales son totalmente independientes, entre sí y con el hypervisor.
- **Portabilidad y recuperación:** gracias a las snapshots.
- **Flexibilidad:** podemos crear las máquinas virtuales con las características de CPU, memoria, disco y red que necesitemos.
- **Agilidad:** la creación de una máquina virtual es un proceso muy rápido.
- **Reducción de costes:** hardware, mantenimiento, energía, ...
- **Eficiencia:** reduciendo el tiempo de inactividad de los servidores.
- **Administración más sencilla.**

Inconvenientes

- **Aumento de los costos iniciales:** software, estudios previos, ...
- **Entorno virtual:** necesidad de aprender a manejarlo. Nuevas herramientas.
- **Menor rendimiento:** Debido a que las máquinas no corren directamente sobre el hardware.
- **Saturamiento:** Un elevado número de VM puede llegar a saturar un servidor.
- **Degradación:** en las máquinas virtuales y en el almacenamiento.

Algunos hipervisores

**CITRIX®
XenServer**

 **Hyper-V**

 **KVM**

 **QEMU**

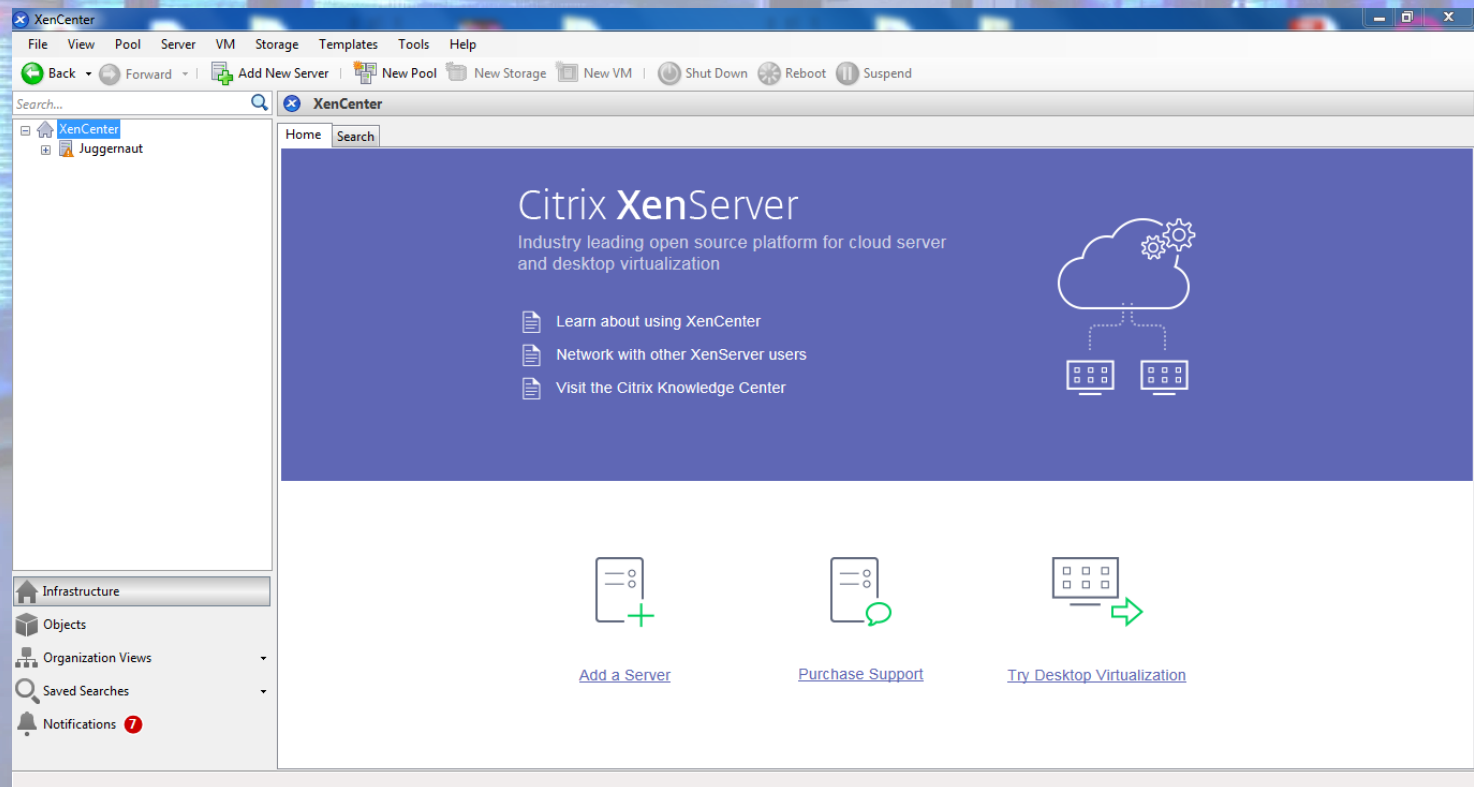



PROXMOX

 **vmware®
ESXi**

XenServer

- **Xen** es un hipervisor de **código abierto** y **gratuito** desarrollado por la Universidad de Cambridge.



DEMO – Servidor Web de «altas prestaciones»

- Balanceador de carga (HAProxy)
- Firewall
- Certificado SSL
- Bases de datos replicadas
- Persistencia en sesiones
- Red interna

jugger.sytes.net

Specs

PC (x1)

- 4C/4T @ 4,3GHz Intel Core I5-4430
 - 8GB RAM
 - 240GB SSD
 - 2x Gigabit NIC
 - 1x 10/100 NIC
-
- 1x XenServer
 - 2x Nodo web

Raspberry PI 3B (x2)

- 4C/4T @ 1,2GHz Broadcom BCM2837
 - 1GB RAM
 - 16GB Flash
 - 1x 10/100 NIC
-
- 1x LoadBalancer (HAProxy)
 - 1x Firewall

WEB



Desarrollo en GitHub

XenCenter

The screenshot displays the XenCenter web interface. The top navigation bar includes menus for File, View, Pool, Server, VM, Storage, Templates, Tools, and Help. Below this is a toolbar with buttons for Back, Forward, Add New Server, New Pool, New Storage, New VM, Shut Down, Reboot, and Suspend. A search bar is located on the left side of the toolbar.

The left sidebar shows a tree view of the XenCenter infrastructure, including a folder for 'Juggernaut' (Unlicensed) and its sub-items: WEB01, WEB02, ANGELMASTERACE, DVD drives, Local storage, and Removable storage. The bottom sidebar contains links to Infrastructure, Objects, Organization Views, Saved Searches, and Notifications.

The main content area displays the 'Server General Properties' for the 'Juggernaut' server. The 'General' tab is selected, showing various system details. The 'Management Interfaces' section lists DNS hostname, Management interface, and IP addresses for WEB02 and WEB01. The 'Memory' section shows available RAM and usage for VMs and XenServer. The 'Version Details' and 'License Details' sections are collapsed. The 'CPUs' section shows details for CPU 0-3, including Vendor, Model, and Speed.

General	
Name:	Juggernaut
Description:	Default install of XenServer
Tags:	<None>
Folder:	<None>
Enabled:	Yes
iSCSI IQN:	iqn.2018-04.com.example:a98d9190
Log destination:	Local
Server uptime:	4 hours 2 minutes
Toolstack uptime:	4 hours 1 minute
UUID:	81a250e6-e02d-4829-bc25-04ee9a4a5498

Management Interfaces	
DNS hostname:	Juggernaut
Management interface:	192.168.1.125
WEB02:	192.168.1.132
WEB01:	192.168.1.131

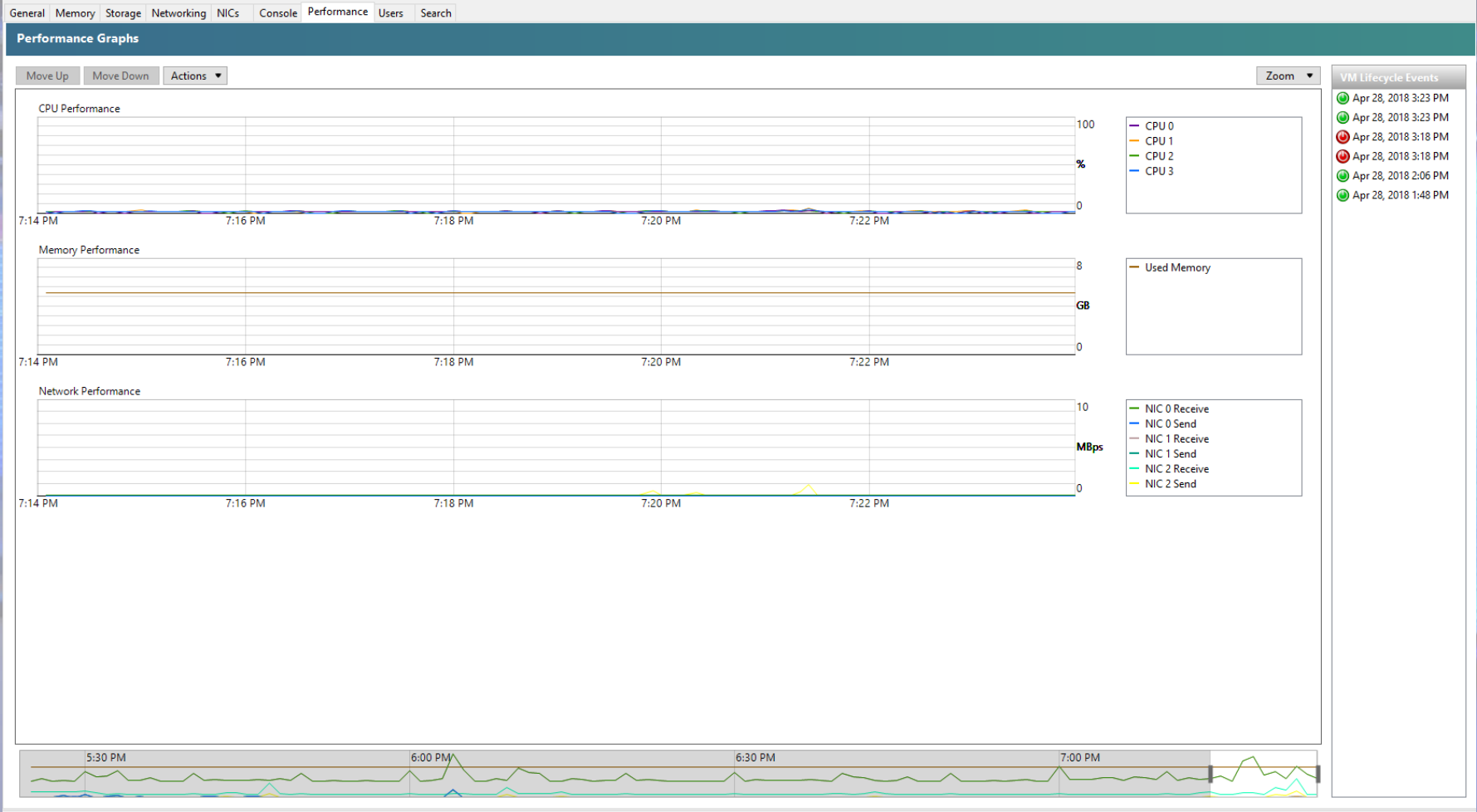
Memory	
Server:	2.8 GB RAM available (7.9 GB total)
VMs:	WEB02: using 2.0 GB WEB01: using 2.0 GB
XenServer:	1.1 GB

Version Details	

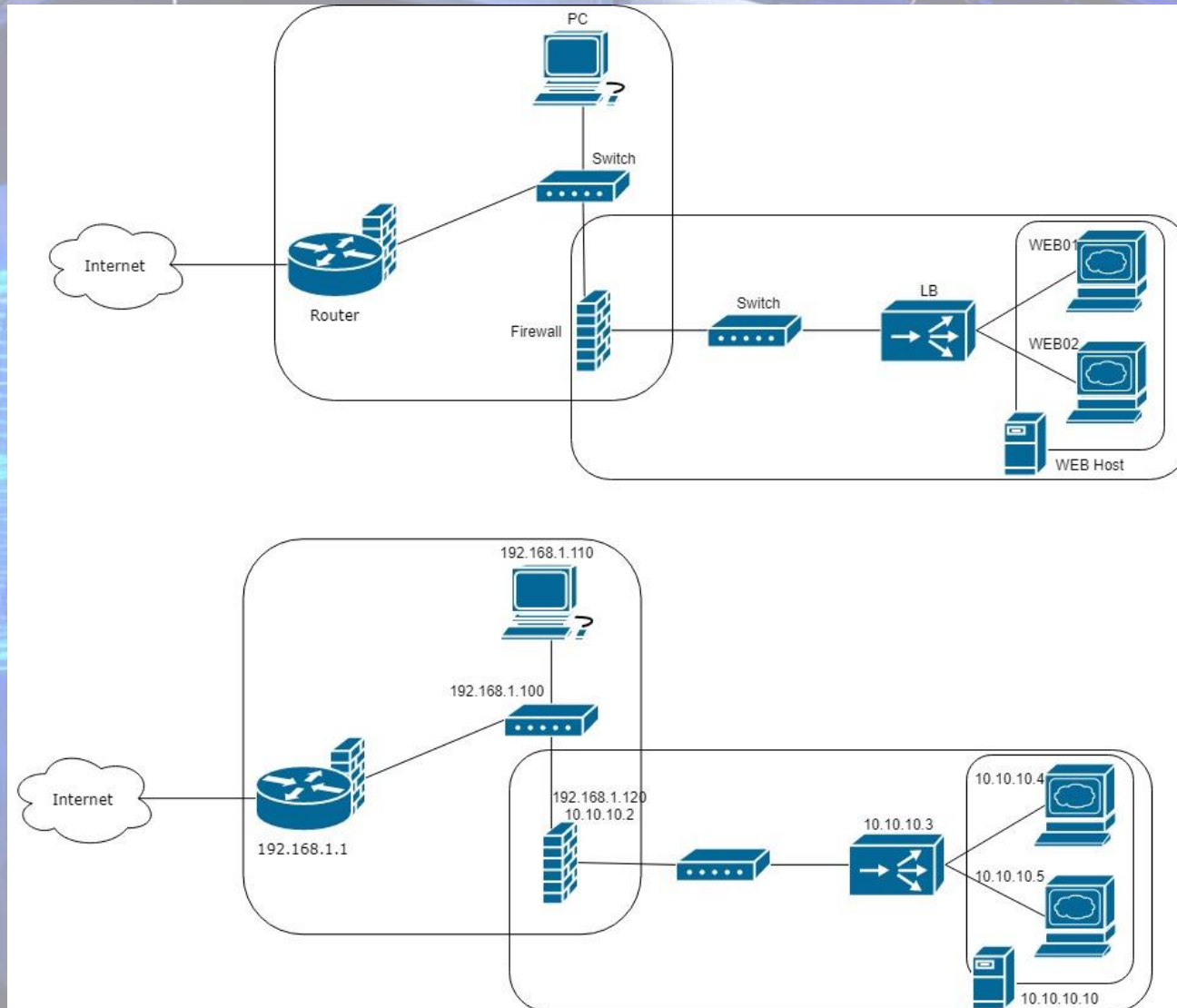
License Details	

CPUs	
CPU 0 - 3:	Vendor: GenuineIntel Model: Intel(R) Core(TM) i5-4430 CPU @ 3.00GHz Speed: 2993 MHz

XenCenter



Networking



Firewall

```
# Borrar todas las reglas que hubiera previamente
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

# Política por defecto (denegar todo)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Permitir forwarding
iptables -P FORWARD ACCEPT

# Permitir loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Permitir puerto 80 (http)
iptables -A INPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT

# Permitir puerto 443 (https)
iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT

# Permitir dns
iptables -A OUTPUT -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp --sport 53 -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 53 -m state --state ESTABLISHED -j ACCEPT

# Redireccionamiento http y https
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to 10.10.10.3:80
iptables -A FORWARD -d 10.10.10.3 -p tcp --dport 80 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to 10.10.10.3:443
iptables -A FORWARD -d 10.10.10.3 -p tcp --dport 443 -j ACCEPT
iptables -t nat -A POSTROUTING -j MASQUERADE
```


HAProxy

```
global
    daemon
    maxconn 1024

defaults
    mode http
    timeout connect 4000
    timeout client 42000
    timeout server 43000

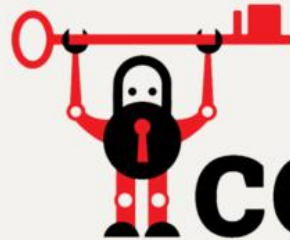
frontend http-in
    bind *:443 ssl crt /etc/haproxy/ssl/jugger.sytes.net.pem
    bind *:80
    default_backend servers

backend servers
    cookie WEB insert
    server web01 10.10.10.4:80 weight 1 maxconn 512 cookie 1 check
    server web02 10.10.10.5:80 weight 1 maxconn 512 cookie 2 check
```

SSL



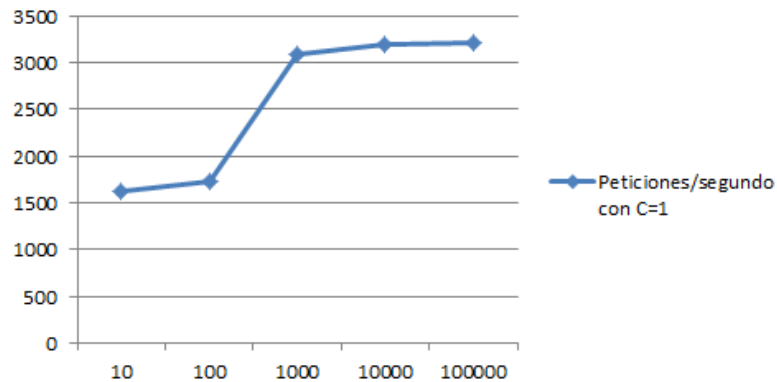
Let's Encrypt



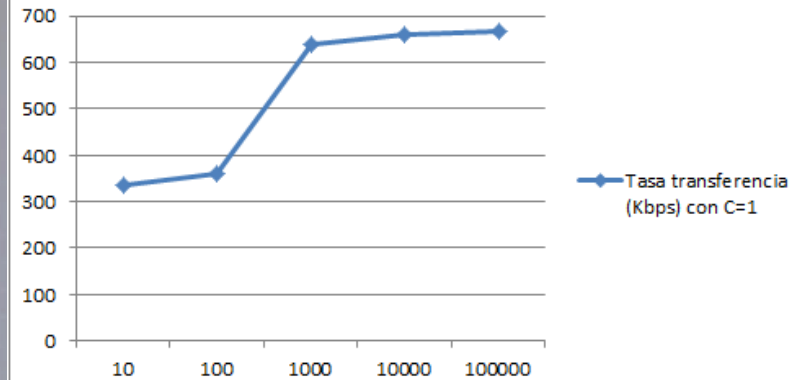
certbot

Benchmarks (AB)

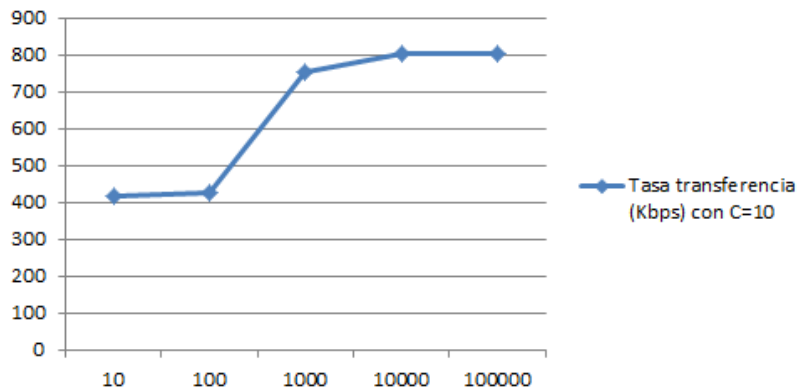
Peticiones/segundo con C=1



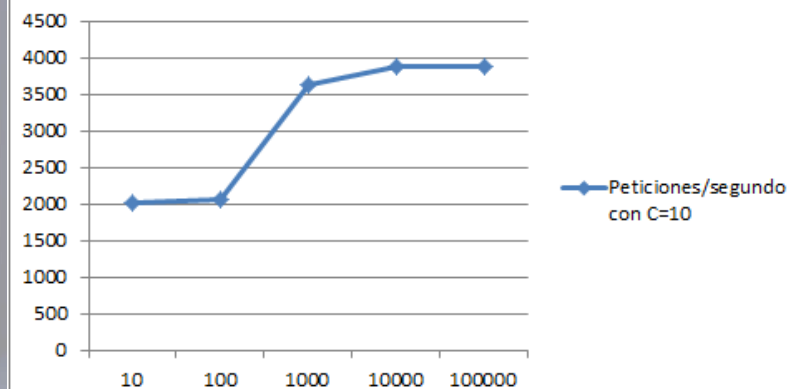
Tasa transferencia (Kbps) con C=1



Tasa transferencia (Kbps) con C=10

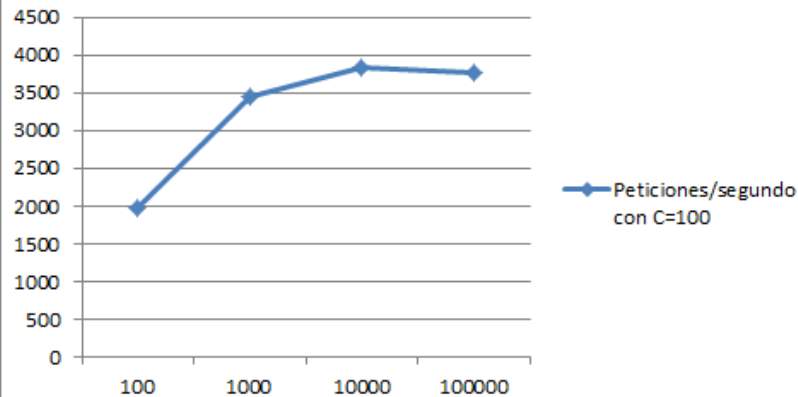


Peticiones/segundo con C=10

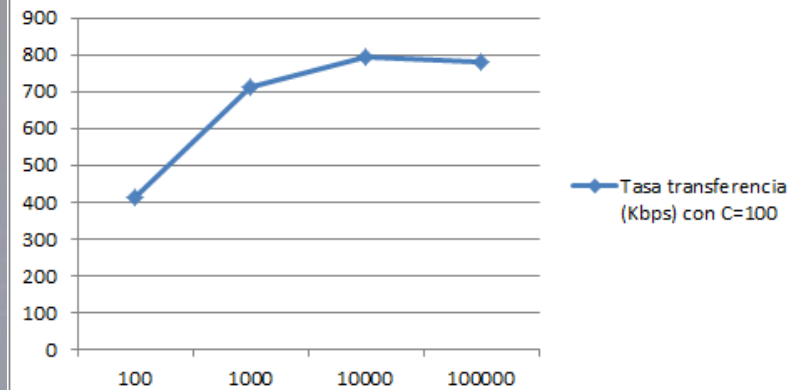


Benchmarks (AB)

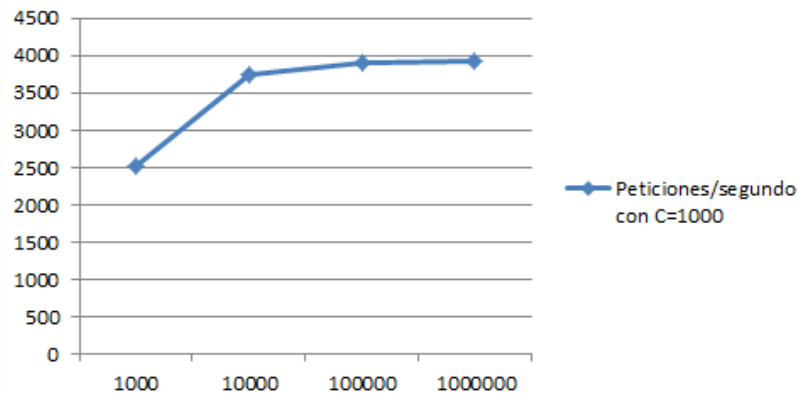
Peticiones/segundo con C=100



Tasa transferencia (Kbps) con C=100



Peticiones/segundo con C=1000



Tasa transferencia (Kbps) con C=1000

