

# **CENTROS DE PROCESAMIENTO DE DATOS**

Práctica 10: Proyecto personal

---

Juan José García Melgar  
Curso 4º, Grupo A - 2018/2019

## Descripción

En esta práctica se trata de utilizar las diversas herramientas, conocimientos y recursos que permitan crear un sistema con las siguientes características:

- Al menos 3 nodos.
- Debe permitir que puedan aumentarse o disminuirse el número de servidores de forma dinámica.
- Algún recurso que permita redundancia en el almacenamiento (GlusterFS) o BBDD redundante (MongoDB, Cassandra).
- Algún mecanismo de control de seguridad (Fail2ban).

Elementos adicionales:

- Monitorización del sistema.
- Balanceo de carga.
- Recursos disponibles que ofrezca el proveedor cloud.
- Diagramas describiendo el sistema: <https://www.yworks.com/products/yed>

## Desarrollo

Para el desarrollo se puede utilizar AWS Educate o algún sistema equivalente.

## Descripción del proyecto

Para todo el proceso, se ha contado con los servicios de Microsoft Azure

<https://azure.microsoft.com/es-es>, que nos brinda todo lo necesario para llevarlo a cabo.

Se ha desarrollado un sistema compuesto por: un clúster de 4 nodos, que pueden aumentarse o disminuirse según necesidad, bajo Ubuntu Server. Incluye un sistema redundante de almacenamiento Gluster File System, con un factor de replicación de 2.

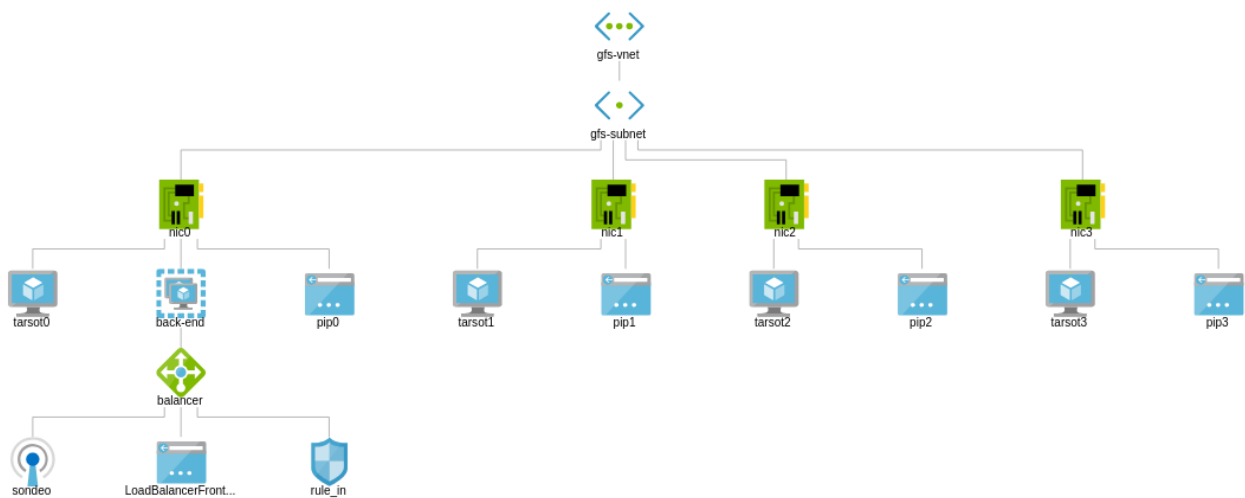
Además, cada nodo tiene una IP pública y 2 discos dispuestos en RAID0.

## Recursos añadidos




















Para dotar a la infraestructura de mayor seguridad, se ha optado por incluir un Firewall de Azure y Fail2ban. Este último, implementado a través de consola, desde los repositorios de Ubuntu. Por otro lado, también se ha optado por añadir un Balanceador de Equilibrio a dicha infraestructura, con un back-end determinado, regla de equilibrio de carga, NAT de entrada y sondeo de estado, a través de un monitor de conexión Network Watcher , que nos permite configurar y realizar el seguimiento de los cambios en la topología de red, la latencia y el alcance de la conexión. Si surge un problema, nos indica porqué se produjo y cómo solucionarlo.










A continuación, se adjuntan algunas capturas, que nos orientan sobre el desarrollo y puesta en marcha de dicha infraestructura:

## Descripción del sistema



## Grupo de recursos utilizados

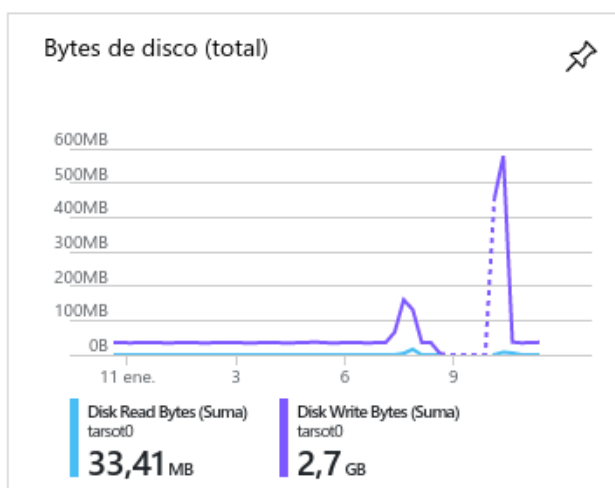
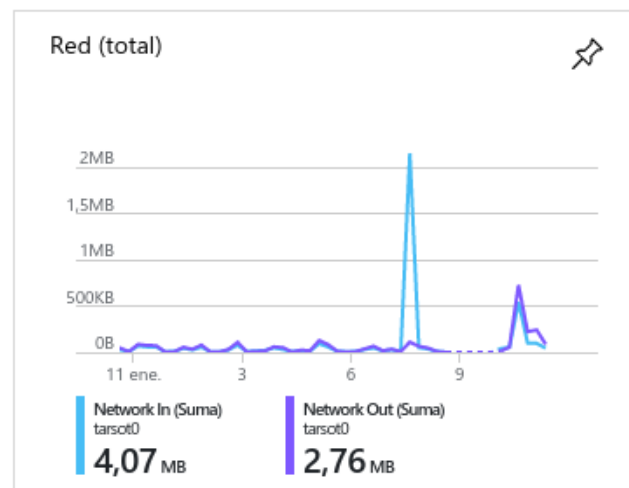
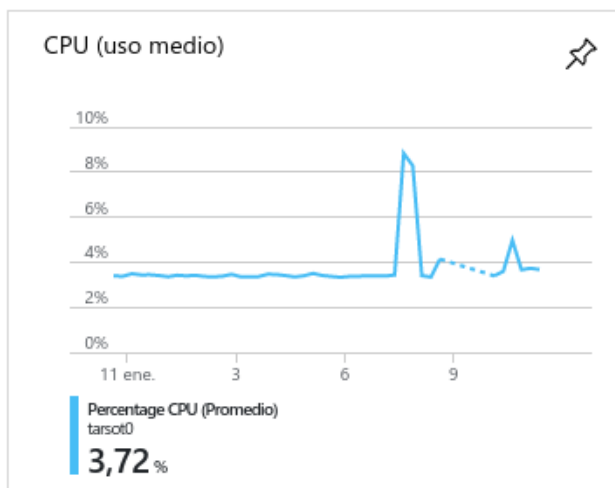
CUENTA DE ALMACENAMIENTO	
<input type="checkbox"/>	 tarsot
DIRECCIÓN IP PÚBLICA	
<input type="checkbox"/>	 azureFirewalls-ip
<input type="checkbox"/>	 pip0
<input type="checkbox"/>	 pip1
<input type="checkbox"/>	 pip2
<input type="checkbox"/>	 pip3
DISCO	
<input type="checkbox"/>	 tarsot0_DataDisk1
<input type="checkbox"/>	 tarsot0_DataDisk2
<input type="checkbox"/>	 tarsot0_OSDisk
<input type="checkbox"/>	 tarsot1_DataDisk1
<input type="checkbox"/>	 tarsot1_DataDisk2
<input type="checkbox"/>	 tarsot1_OSDisk
<input type="checkbox"/>	 tarsot2_DataDisk1
<input type="checkbox"/>	 tarsot2_DataDisk2
<input type="checkbox"/>	 tarsot2_OSDisk
<input type="checkbox"/>	 tarsot3_DataDisk1
<input type="checkbox"/>	 tarsot3_DataDisk2
<input type="checkbox"/>	 tarsot3_OSDisk
EQUILIBRADOR DE CARGA	
<input type="checkbox"/>	 balancer

INTERFAZ DE RED	
<input type="checkbox"/>	 nic0
<input type="checkbox"/>	 nic1
<input type="checkbox"/>	 nic2
<input type="checkbox"/>	 nic3
MÁQUINA VIRTUAL	
<input type="checkbox"/>	 tarsot0
<input type="checkbox"/>	 tarsot1
<input type="checkbox"/>	 tarsot2
<input type="checkbox"/>	 tarsot3
RED VIRTUAL	
<input type="checkbox"/>	 gfs-vnet

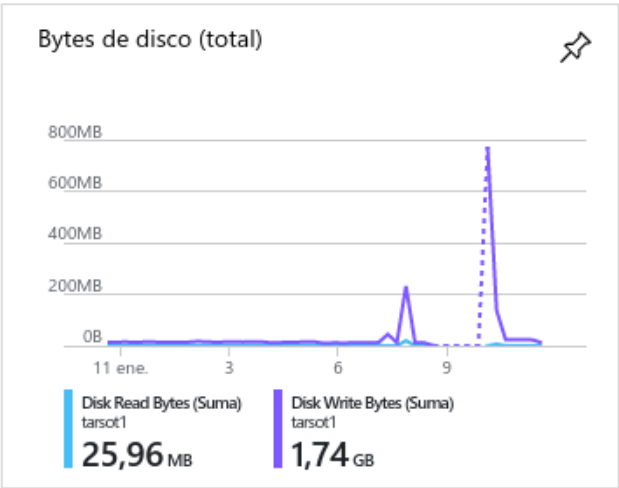
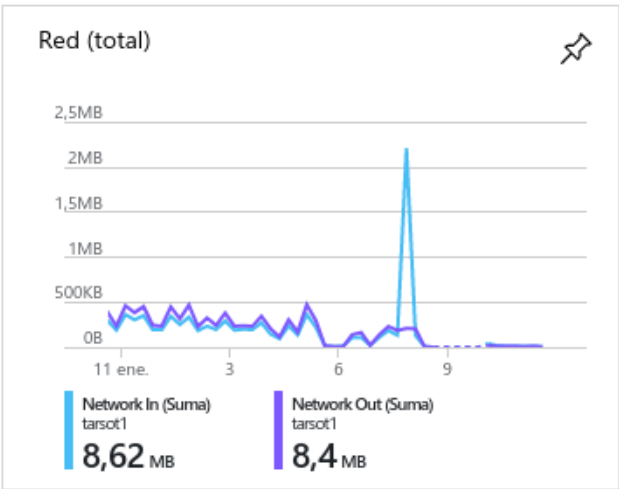
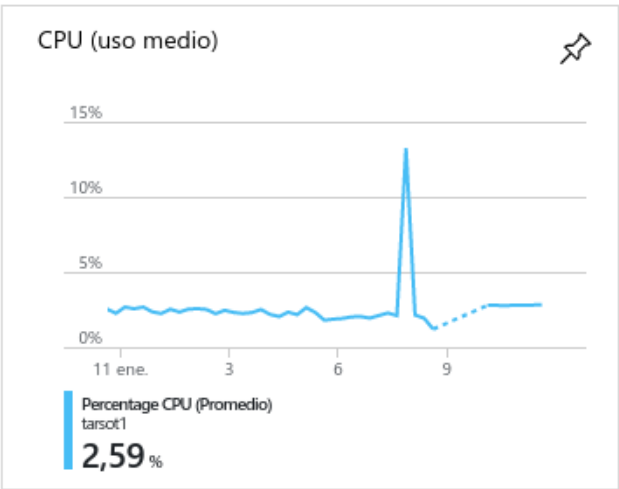
## Nodos

A modo de ejemplo, se detallan algunos parámetros de monitorización de los servidores, durante un periodo de actividad equivalente a doce horas:

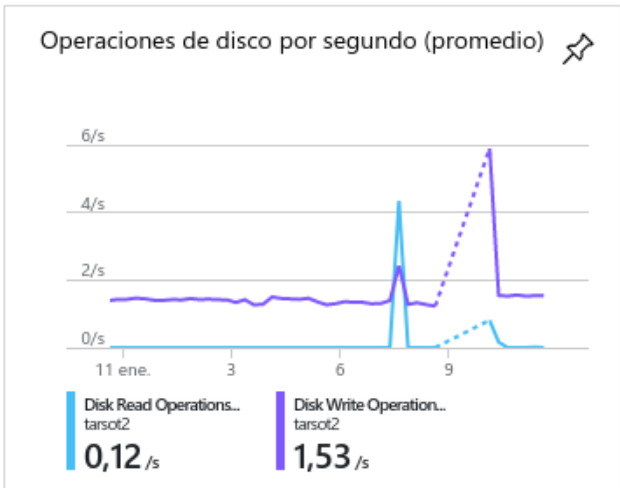
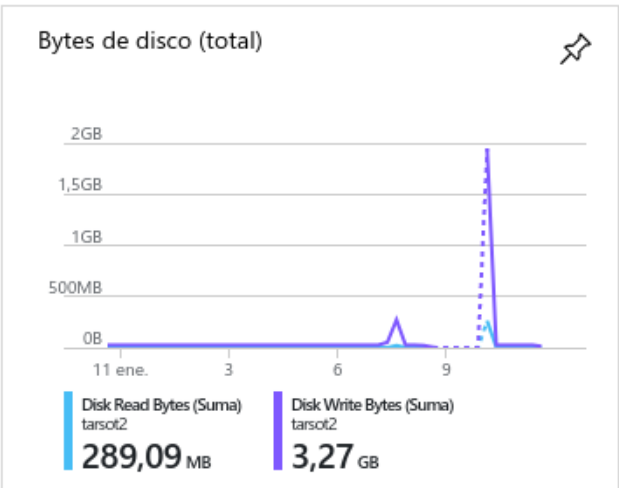
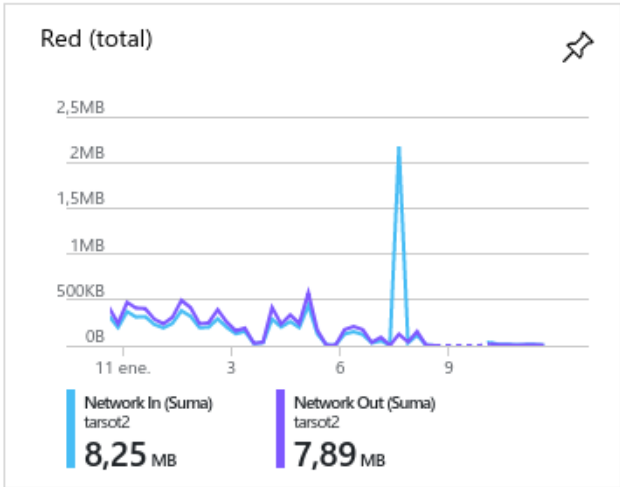
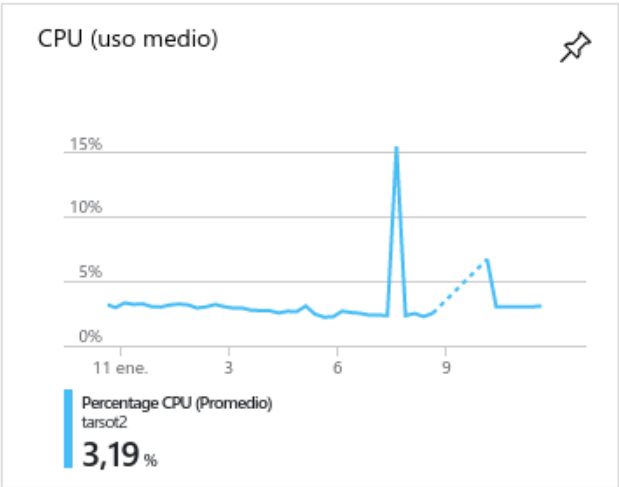
### Servidor 1 (tarsot0)



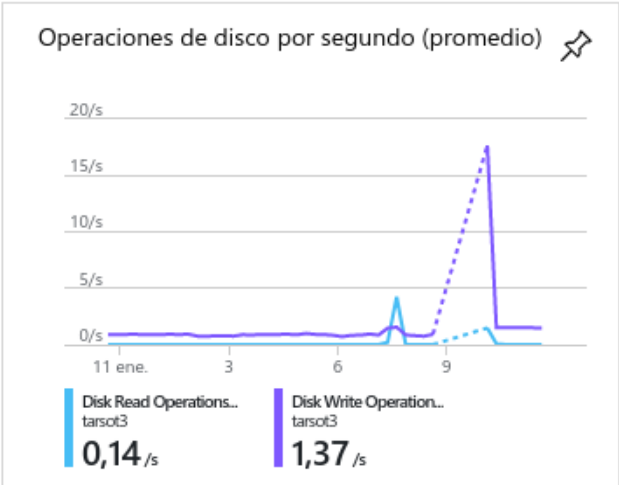
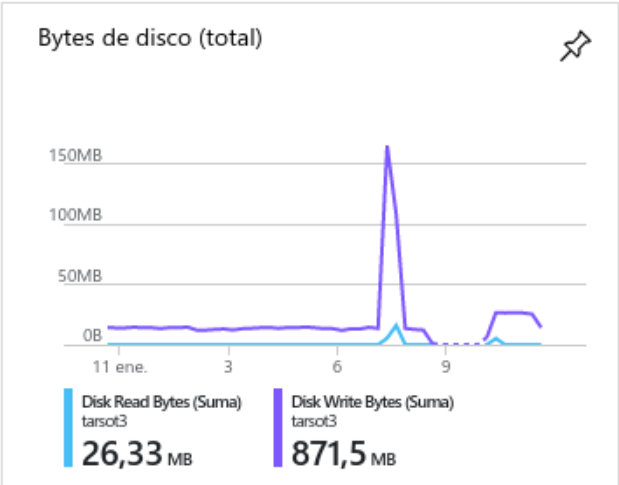
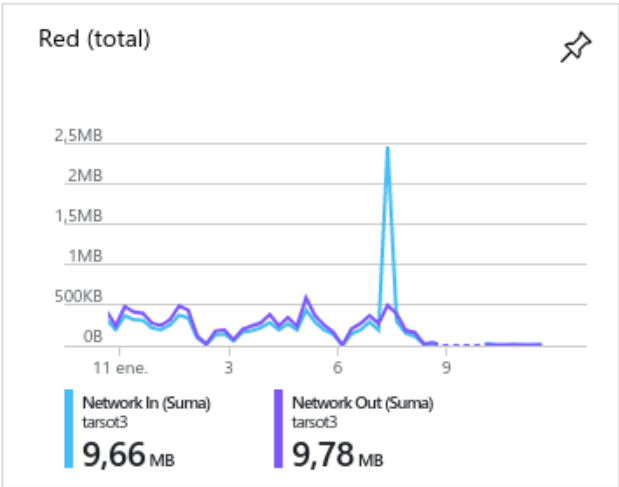
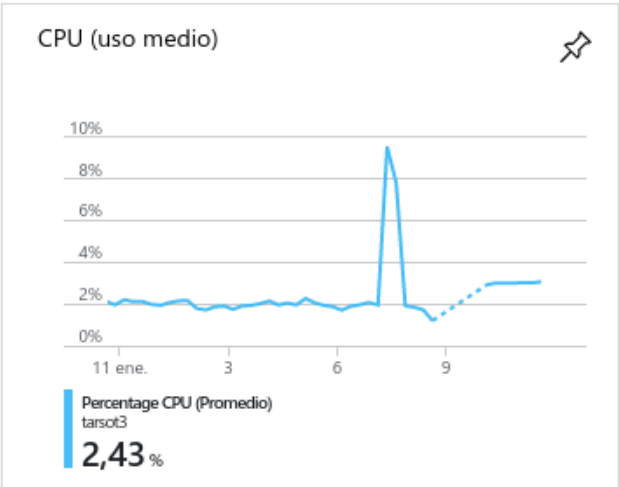
Servidor 2 (tarsot1)



Servidor 3 (tarsot2)



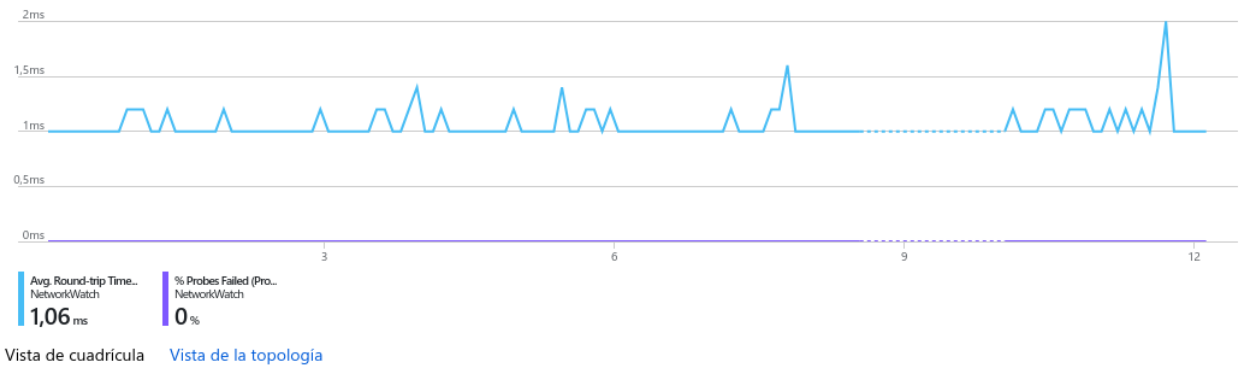
Servidor 4 (tarsot3)





Network watcher

Error de promedio de tiempo de ida y vuelta y porcentaje de sondeos



Salto

NOMBRE	DIRECCIÓN IP	ESTADO	DIRECCIÓN IP DEL PRÓXIM...	RTT DESDE ORIGEN (MS)
tarsot0	10.0.0.8		10.0.0.9	2
tarsot1	10.0.0.9		-	-

Fail2ban

```
tarsot@tarsot0:~$ ps aux | grep -l fail2ban | grep -v grep
root      6748  0.2  0.7 488616 13184 ?        Sl    09:43   0:03 /usr/bin/python /usr/bin/fail2ban-server -b -s /var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid
```

```
INFO    Changed logging target to /var/log/fail2ban.log for Fail2ban v0.8.11
INFO    Creating new jail 'ssh'
INFO    Jail 'ssh' uses pyinotify
INFO    Initiated 'pyinotify' backend
INFO    Added logfile = /var/log/auth.log
INFO    Set maxRetry = 2
INFO    Set findtime = 600
INFO    Set banTime = 600
INFO    Creating new jail 'dropbear'
INFO    Jail 'dropbear' uses pyinotify
INFO    Initiated 'pyinotify' backend
INFO    Added logfile = /var/log/auth.log
INFO    Set maxRetry = 2
INFO    Set findtime = 600
INFO    Set banTime = 600
INFO    Creating new jail 'ssh-ddos'
INFO    Jail 'ssh-ddos' uses pyinotify
INFO    Initiated 'pyinotify' backend
INFO    Added logfile = /var/log/auth.log
INFO    Set maxRetry = 2
INFO    Set findtime = 600
INFO    Set banTime = 600
INFO    Jail 'ssh' started
INFO    Jail 'dropbear' started
INFO    Jail 'ssh-ddos' started
```