**integrapro**

**Puertos del Estado**

**Departamento de Informática**

**CONTROL DE DIFUSIÓN****[[1]](#footnote-2)**

|  |
| --- |
| RESPONSABLE: Departamento de Informática |
| AUTOR/ES: Satec SA |
| DISTRIBUCIÓN: Departamento de Informática |

Índice

**Contenido**

[CONTROL DE DIFUSIÓN 3](#__RefHeading___Toc1039_2644738205)

[1 Descripción 5](#__RefHeading___Toc1041_2644738205)

[2 Acceso 5](#__RefHeading___Toc1107_434703637)

[3 Hardware 5](#__RefHeading___Toc8449_1165651232)

[Sistema Operativo 5](#__RefHeading___Toc12623_937315845)

[3.1 Versión: 5](#__RefHeading___Toc1070_434703637)

[3.2 Seguridad 6](#__RefHeading___Toc8451_1165651232)

[3.2.1 Firewall 6](#__RefHeading___Toc8453_1165651232)

[3.2.2 Selinux 6](#__RefHeading___Toc8455_1165651232)

[3.2.3 Usuarios 6](#__RefHeading___Toc12625_937315845)

[3.2.4 Grupos 6](#__RefHeading___Toc12627_937315845)

[3.2.5 Integracion AD 6](#__RefHeading___Toc12629_937315845)

[3.2.6 Sudo 7](#__RefHeading___Toc12631_937315845)

[3.2.7 Configuración ssh server. 7](#__RefHeading___Toc12633_937315845)

[3.3 Almacenamiento 7](#__RefHeading___Toc8457_1165651232)

[3.3.1 Particiones 7](#__RefHeading___Toc8459_1165651232)

[3.3.2 Punto de montaje 7](#__RefHeading___Toc8461_1165651232)

[3.4 RED 7](#__RefHeading___Toc8508_1165651232)

[3.4.1 Interfaz de red 7](#__RefHeading___Toc8510_1165651232)

[3.4.2 Rutas de red 7](#__RefHeading___Toc12635_937315845)

[3.4.3 Resolucion de nombre en el DNS 7](#__RefHeading___Toc8512_1165651232)

[3.4.4 Jobs programados 8](#__RefHeading___Toc12637_937315845)

[3.5 Procesos 8](#__RefHeading___Toc12639_937315845)

[3.5.1 Procesos importantes. 8](#__RefHeading___Toc12641_937315845)

[3.5.2 Puertos activos. 8](#__RefHeading___Toc12643_937315845)

[3.5.3 Conexiones establecidas. 8](#__RefHeading___Toc12645_937315845)

[3.6 Nagios 8](#__RefHeading___Toc1043_2644738205)

[4 Software Instalado 9](#__RefHeading___Toc24961_937315845)

[5 Procedimientos 9](#__RefHeading___Toc24963_937315845)

# Descripción

El presente documento detalla la instalación y configuración de un nuevo servidor para el departamento de TI denominado integrapro.puertos.es (a partir de ahora lo identificaremos como integrapro).

Este nuevo servidor es una máquina virtual alojada en el vcenter “vcenter5.puertos.es”, y se ha creado a partir de la plantilla de Red Hat Enterprise Linux Server 7.6 (Maipo) ubicada en el entorno virtual. Adicionalmente, se ha realizado toda post configuración (ntp, nrpe,…..) a través de ansible.

# Acceso

Nombre del equipo: integrapro.puertos.es

IP interna: 172.20.22.238

Credenciales: usuario sistemas del Keepass

# Hardware

El servidor desponto tiene el siguiente hardware virtual:

* CPU: 2 vCPUS.
* Memoria: 1838 MB.
* Discos: 2 discos

NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT

fd0 2:0 1 4K 0 disk   
  
sda 8:0 0 30G 0 disk

# Sistema Operativo

## Versión:

Red Hat Enterprise Linux Server release 7.6 (Maipo)

## Seguridad

### Firewall

Se deshabilita el firewall para este servidor.

Chain INPUT (policy ACCEPT)  
  
target prot opt source destination   
  
  
  
Chain FORWARD (policy ACCEPT)  
  
target prot opt source destination   
  
  
  
Chain OUTPUT (policy ACCEPT)  
  
target prot opt source destination

### Selinux

Se pone en modo disabled Selinux.

SELinux status: disabled

### Usuarios

Estos son los usuarios locales del servidor:

root:x:0:0:root:/root:/bin/bash  
  
bin:x:1:1:bin:/bin:/sbin/nologin  
  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
  
sync:x:5:0:sync:/sbin:/bin/sync  
  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
  
halt:x:7:0:halt:/sbin:/sbin/halt  
  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
  
operator:x:11:0:operator:/root:/sbin/nologin  
  
games:x:12:100:games:/usr/games:/sbin/nologin  
  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
  
nobody:x:99:99:Nobody:/:/sbin/nologin  
  
systemd-bus-proxy:x:999:997:systemd Bus Proxy:/:/sbin/nologin  
  
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin  
  
dbus:x:81:81:System message bus:/:/sbin/nologin  
  
polkitd:x:998:996:User for polkitd:/:/sbin/nologin  
  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin  
  
postfix:x:89:89::/var/spool/postfix:/sbin/nologin  
  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
  
chrony:x:997:995::/var/lib/chrony:/sbin/nologin  
  
sistemas:x:2000:

### Grupos

root:x:0:  
  
bin:x:1:  
  
daemon:x:2:  
  
sys:x:3:  
  
adm:x:4:  
  
tty:x:5:  
  
disk:x:6:  
  
lp:x:7:  
  
mem:x:8:  
  
kmem:x:9:  
  
wheel:x:10:sistemas  
  
cdrom:x:11:  
  
mail:x:12:postfix  
  
man:x:15:  
  
dialout:x:18:  
  
floppy:x:19:  
  
games:x:20:  
  
tape:x:30:  
  
video:x:39:  
  
ftp:x:50:  
  
lock:x:54:  
  
audio:x:63:  
  
nobody:x:99:  
  
users:x:100:  
  
utmp:x:22:  
  
utempter:x:35:  
  
ssh\_keys:x:999:  
  
input:x:998:  
  
systemd-journal:x:190:  
  
systemd-bus-proxy:x:997:  
  
systemd-network:x:192:  
  
dbus:x:81:  
  
polkitd:x:996:  
  
tss:x:59:  
  
dip:x:40:  
  
postdrop:x:90:  
  
postfix:x:89:  
  
sshd:x:74:  
  
chrony:x:995:  
  
sistemas:x:2000:sistemas  
  
unbound:x:994:  
  
saslauth:x:76:  
  
cgred:x:993:  
  
libvirt:x:992:  
  
ntp:x:38:  
  
nagios:x:991:nrpe  
  
nrpe:x:990:  
  
printadmin:x:989:  
  
rpc:x:32:  
  
admins:x:10000:  
  
sssd:x:988:  
  
jboss:x:10001:  
  
appusers:x:10002:agarcia.prodevelop

### Integracion AD

PUERTOS.ES  
  
 type: kerberos  
  
 realm-name: PUERTOS.ES  
  
 domain-name: puertos.es  
  
 configured: kerberos-member  
  
 server-software: active-directory  
  
 client-software: sssd  
  
 required-package: oddjob  
  
 required-package: oddjob-mkhomedir  
  
 required-package: sssd  
  
 required-package: adcli  
  
 required-package: samba-common-tools  
  
 login-formats: %U  
  
 login-policy: allow-permitted-logins  
  
 permitted-logins:   
  
 permitted-groups:

### Sudo

Defaults !visiblepw  
  
Defaults always\_set\_home  
  
Defaults env\_reset  
  
Defaults env\_keep = "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS\_COLORS"  
  
Defaults env\_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC\_ADDRESS LC\_CTYPE"  
  
Defaults env\_keep += "LC\_COLLATE LC\_IDENTIFICATION LC\_MEASUREMENT LC\_MESSAGES"  
  
Defaults env\_keep += "LC\_MONETARY LC\_NAME LC\_NUMERIC LC\_PAPER LC\_TELEPHONE"  
  
Defaults env\_keep += "LC\_TIME LC\_ALL LANGUAGE LINGUAS \_XKB\_CHARSET XAUTHORITY"  
  
Defaults secure\_path = /sbin:/bin:/usr/sbin:/usr/bin  
  
root ALL=(ALL) ALL  
  
%wheel ALL=(ALL) NOPASSWD: ALL  
  
%admins ALL=(ALL) NOPASSWD: ALL  
  
%linuxadmins ALL=(ALL) NOPASSWD: ALL  
  
%appusers ALL=(ALL) NOPASSWD: ALL

### Configuración ssh server.

HostKey /etc/ssh/ssh\_host\_rsa\_key  
  
HostKey /etc/ssh/ssh\_host\_ecdsa\_key  
  
HostKey /etc/ssh/ssh\_host\_ed25519\_key  
  
SyslogFacility AUTHPRIV  
  
AuthorizedKeysFile .ssh/authorized\_keys  
  
PasswordAuthentication yes  
  
ChallengeResponseAuthentication no  
  
GSSAPIAuthentication yes  
  
GSSAPICleanupCredentials no  
  
UsePAM yes  
  
X11Forwarding yes  
  
AcceptEnv LANG LC\_CTYPE LC\_NUMERIC LC\_TIME LC\_COLLATE LC\_MONETARY LC\_MESSAGES  
  
AcceptEnv LC\_PAPER LC\_NAME LC\_ADDRESS LC\_TELEPHONE LC\_MEASUREMENT  
  
AcceptEnv LC\_IDENTIFICATION LC\_ALL LANGUAGE  
  
AcceptEnv XMODIFIERS  
  
Subsystem sftp /usr/libexec/openssh/sftp-server  
  
AllowGroups admins linuxadmins appusers

## Almacenamiento

### Particiones

Filesystem Type 1K-blocks Used Available Use% Mounted on  
  
/dev/mapper/vg0-root xfs 10475520 1655488 8820032 16% /  
  
devtmpfs devtmpfs 929356 0 929356 0% /dev  
  
tmpfs tmpfs 941236 0 941236 0% /dev/shm  
  
tmpfs tmpfs 941236 9064 932172 1% /run  
  
tmpfs tmpfs 941236 0 941236 0% /sys/fs/cgroup  
  
/dev/mapper/vg0-srv xfs 1943552 32992 1910560 2% /srv  
  
/dev/mapper/vg0-home xfs 1939456 33120 1906336 2% /home  
  
/dev/mapper/vg0-tmp xfs 975524 33128 942396 4% /tmp  
  
/dev/sda1 xfs 1038336 225552 812784 22% /boot  
  
/dev/mapper/vg0-opt xfs 1939456 328804 1610652 17% /opt  
  
/dev/mapper/vg0-var xfs 1943552 664372 1279180 35% /var  
  
tmpfs tmpfs 188248 0 188248 0% /run/user/2000

### Punto de montaje

/dev/mapper/vg0-root / xfs defaults 0 0  
  
UUID=5d1ab055-920f-4969-91a1-7cdbaf64651c /boot xfs defaults 0 0  
  
/dev/mapper/vg0-home /home xfs defaults 0 0  
  
/dev/mapper/vg0-opt /opt xfs defaults 0 0  
  
/dev/mapper/vg0-srv /srv xfs defaults 0 0  
  
/dev/mapper/vg0-tmp /tmp xfs defaults 0 0  
  
/dev/mapper/vg0-var /var xfs defaults 0 0  
  
/dev/mapper/vg0-swap swap swap defaults 0 0

## RED

### Interfaz de red

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
  
 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
  
 inet 127.0.0.1/8 scope host lo  
  
 valid\_lft forever preferred\_lft forever  
  
 inet6 ::1/128 scope host   
  
 valid\_lft forever preferred\_lft forever  
  
2: ens192: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc mq state UP group default qlen 1000  
  
 link/ether 00:50:56:95:12:aa brd ff:ff:ff:ff:ff:ff  
  
 inet 172.20.22.238/23 brd 172.20.23.255 scope global noprefixroute ens192  
  
 valid\_lft forever preferred\_lft forever  
  
 inet6 fe80::250:56ff:fe95:12aa/64 scope link noprefixroute   
  
 valid\_lft forever preferred\_lft forever

### Rutas de red

default via 172.20.22.1 dev ens192 proto static metric 100   
  
172.20.22.0/23 dev ens192 proto kernel scope link src 172.20.22.238 metric 100

### Resolucion de nombre en el DNS

# Generated by NetworkManager  
  
search puertos.es  
  
nameserver 172.20.22.150  
  
nameserver 172.20.22.16  
  
nameserver 172.20.22.17

### Jobs programados

Sin configurar

## Procesos

### Procesos importantes.

UID PID PPID C STIME TTY TIME CMD  
  
jboss 4989 4799 10 15:26 ? 00:00:13 java -D[Standalone] -server -Xms64m -Xmx512m -XX:MetaspaceSize=96M -XX:MaxMetaspaceSize=256m -Djava.net.preferIPv4Stack=true -Djboss.modules.system.pkgs=org.jboss.byteman -Djava.awt.headless=true -Dorg.jboss.boot.log.file=/opt/wildfly-10.0.0.Final/standalone/log/server.log -Dlogging.configuration=file:/opt/wildfly-10.0.0.Final/standalone/configuration/logging.properties -jar /opt/wildfly-10.0.0.Final/jboss-modules.jar -mp /opt/wildfly-10.0.0.Final/modules org.jboss.as.standalone -Djboss.home.dir=/opt/wildfly-10.0.0.Final -Djboss.server.base.dir=/opt/wildfly-10.0.0.Final/standalone  
  
root 5184 1 1 15:27 ? 00:00:01 /usr/bin/python /usr/bin/virt-who  
  
root 1 0 1 15:26 ? 00:00:01 /usr/lib/systemd/systemd --switched-root --system --deserialize 22  
  
root 2357 1 0 15:26 ? 00:00:00 /usr/lib/systemd/systemd-journald  
  
root 2377 1 0 15:26 ? 00:00:00 /usr/lib/

### Puertos activos.

LISTEN 0 128 \*:111 \*:\*   
  
LISTEN 0 128 172.20.22.238:8080 \*:\*   
  
LISTEN 0 128 \*:22 \*:\*   
  
LISTEN 0 100 127.0.0.1:25 \*:\*   
  
LISTEN 0 5 \*:5666 \*:\*   
  
LISTEN 0 50 172.20.22.238:9990 \*:\*   
  
LISTEN 0 128 :::111 :::\*   
  
LISTEN 0 128 :::22 :::\*   
  
LISTEN 0 100 ::1:25 :::\*   
  
LISTEN 0 5 :::5666 :::\*

### Conexiones establecidas.

ESTAB 0 0 172.20.22.238:46674 172.20.22.16:389   
  
ESTAB 0 112 172.20.22.238:22 172.20.12.46:40946   
  
ESTAB 0 0 172.20.22.238:39736 172.20.22.17:3268   
  
ESTAB 0 0 172.20.22.238:39494 172.20.22.100:443

## Nagios

Para tener monitorizado el servidor se ha configurado lo siguiente en el fichero /etc/nagios/nrpe.cfg :

log\_facility=daemon  
  
debug=0  
  
pid\_file=/var/run/nrpe/nrpe.pid  
  
server\_port=5666  
  
nrpe\_user=nrpe  
  
nrpe\_group=nrpe  
  
allowed\_hosts=127.0.0.1,::1  
  
dont\_blame\_nrpe=0  
  
allow\_bash\_command\_substitution=0  
  
command\_timeout=60  
  
connection\_timeout=300  
  
command[check\_users]=/usr/lib64/nagios/plugins/check\_users -w 5 -c 10  
  
command[check\_load]=/usr/lib64/nagios/plugins/check\_load -r -w .15,.10,.05 -c .30,.25,.20  
  
command[check\_hda1]=/usr/lib64/nagios/plugins/check\_disk -w 20% -c 10% -p /dev/hda1  
  
command[check\_zombie\_procs]=/usr/lib64/nagios/plugins/check\_procs -w 5 -c 10 -s Z  
  
command[check\_total\_procs]=/usr/lib64/nagios/plugins/check\_procs -w 150 -c 200  
  
include\_dir=/etc/nrpe.d/

# Software Instalado

# Procedimientos

1. *Este documento y cualquier parte de su contenido es propiedad de Puertos del Estado. Ninguna parte de este documento puede ser ni reproducido ni transmitido de ninguna manera, o almacenado en un sistema recuperable, o por otros medios, mecánico, fotográfico, electrónico, o de otro modo sin el permiso explícito del responsable.* [↑](#footnote-ref-2)