

ASORC

**Administración de sistemas operativos
en redes de computadores**

LINUX Family

CentOS 7 Based

Disk Partitioning

Aim: Create/Add Hard disk partitions.

Install: yum -y install e2fsprogs

Practical case:

- fdisk /dev/sdb
 - m: menu
 - n: new partition (p: primary partition)
 - t: type file system (L: available types)
 - p: previsualize new partition table
 - w: write new partition table to disk
- mount /dev/sdb1 /disco2

Test: fdisk -l

Network configuration

Aim: Assign IP address static/dynamic

Configuration file: /etc/sysconfig/network-scripts/enp0s8

Practical case:

- Static IP : BOOTPROTO=static
 IPADDR=192.168.2.2
 NETMASK=255.255.255.0
 GATEWAY=192.168.2.1
 DNS1=8.8.8.8
- Dynamic IP : BOOTPROTO=dhcp
- Recommended: NM_CONTROLLED=no

Test: ifconfig

Repositories

Aim: Establish software repository source

Install: yum –y install epel-release

Configuration file: /etc/yum.repos.d/epel.repo

- enabled = 1

Practical case:

update: yum repolist

Other repositories: nux-dextop, rpmforge...

Start/Restart/Stop services

Aim: Start/Restart/Stop the deamon that controls the service.
Usually, the name of the service references the deamon:**sshd**

Practical case: ‘**sshd**’ service

- Start: **systemctl start sshd**
- Stop: **systemctl stop sshd**

Activate to start with the system

- Enable: **systemctl enable sshd**
- Disable: **systemctl disable sshd**
- Status: **systemctl status sshd**

Test: **netstat -lp**

SSH

Aim: Remote access to the system (secure way).

Install: Installed by default.

Port: 22 (Port change is recommended)

Configuration file: /etc/ssh/sshd_config

- Port change: Port 1234
- Update protocol: Protocol 2
- Authorized users: AllowUsers marc
- Root Access: PermitRootLogin no

Practical case:

- systemctl restart sshd

Test: ssh -p 1234 marc@192.168.2.2

VNC Server

Aim: Remote graphical access. NO secure protocol.

Install: yum -y install tigervnc-server

Port: 5901

Practical case:

- cp /lib/systemd/system/vncserver@.service \
/etc/systemd/system/vncserver@:1.service
- /etc/systemd/system/vncserver@\:1.service
 - Modificar <USER>: marc
- systemctl start vncserver@:1.service

Test: vncview marc@192.168.2.2:5901

RDP Server

Aim: Remote graphical access. No secure protocol

Install: yum install xrdp

Port: 3389

Practical case:

- systemctl start xrdp

Test: xfreerdp marc@192.168.2.2:3389

NX

Aim: Remote graphical access. Secure access through ssh.

Install: yum -y install x2goserver

Port: 22

Practical case:

- X2godbadmin --createdb
- x2gocleansession

Test: x2goclient

DNS

Aim: Obtain IP through internet domain name.

Install: yum install bind

Port: 53

Configuration file: /etc/named.conf

Practical case:

- Network name: network.com
- IP address: 192.168.2.0/24
- Nodes:
 - server: 192.168.2.100
 - nodeA: 192.168.2.101

Test: nslookup nodoA

Configuration File

/etc/named.conf

```
options {  
    listen-on port 53 { 127.0.0.1; 192.168.2.0/24 };  
    directory "/var/named";  
    forwarders { 193.145.233.5; 8.8.8.8; };  
};  
  
zone "network.net" IN {  
    type master;  
    file "network.zone"; };  
  
zone "2.168.192.in-addr.arpa" IN {  
    type master;  
    file "reverse.zone"; };
```

Configuration file

/var/named/network.zone

```
$TTL 86400
@ IN SOA network.net root.network.net.
(150115 28800 7200 604800 86400)
        IN NS      servidor.network.net.
        IN MX 10  servidor.network.net.
servidor.network.net.    IN A 192.168.2.100
nodoA.network.net.     IN A 192.168.2.101
```

/var/named/reverse.zone

```
$TTL 86400
@ IN SOA network.net. root.network.net.
(150115 28800 7200 604800 86400)
        IN NS servidor.network.net.
100.2.168.192.in-addr.arpa. IN PTR servidor.network.net.
101.2.168.192.in-addr.arpa. IN PTR nodoA.network.net.
```

DHCP

Aim: Serve IP address to any client in the network dynamically

Install: yum install dhcp

Port: 67-68 UDP

File: /etc/dhcp/dhcpd.conf

Practical Case:

- Network name: network.com
- Network address: 192.168.2.0/24
- Nodes:
 - Dhcpc server: 192.168.2.100
 - Dns server: 192.168.2.100
 - gateway: 192.168.2.1
 - NodeA: 192.168.2.101

Configuration file

/etc/dhcp/dhcpd.conf

```
shared-network network.net {  
    subnet 192.168.2.0 netmask 255.255.255.0 {  
        option routers 192.168.2.1;  
        option subnet-mask 255.255.255.0;  
        option broadcast-address 192.168.2.255;  
        option domain-name-servers 192.168.2.100;  
        range 192.168.2.201 192.168.2.209;  
    } }  
  
host learn {  
    option host-name "nodoA.network.net";  
    hardware ethernet 00:25:d3:66:63:b3;  
    fixed-address 192.168.2.101; }
```

NFS. Network File System

Aim: Share folders in local network.

Install: yum -y install nfs-utils

Port: 2049

Configuration file: /etc/exports

/folder_to_share 192.168.2.0/24(rw,no_root_squash)

Practical case:

- systemctl start nfs-server

Test:

- showmount -e 192.168.2.2
- mount -t nfs 192.168.2.2:/folder_to_share /mount_point

SAMBA. SMB

Aim: Share folders in the network using SMB protocol

Install: yum -y install samba samba-client samba-common

Port: 137-139

Configuration file: /etc/samba/smb.conf

Practical case:

- usuario del servicio: smbpasswd -a marc
- Start service: systemctl start nmb
systemctl start smb

Test:

- smbclient //192.168.2.2:/samba -U marc
- mount -t cifs -o username=marc //192.168.2.2/samba /mount_point

Configuration file

/etc/samba/smb.conf:

```
workgroup = admin  
netbios name = admin  
server string = Mi servidor SAMBA  
hosts allow = 192.168.2.  
  
[samba]  
comment = Shared Folder  
path = /samba  
# Hiden files  
hide dot file = Yes  
# Trash  
vfs objects = recycle  
recycle:repository = Recycle Bin
```

FTP server. File Transfer Protocol

Aim: Allow file transfer between server and client.

Install: yum -y install vsftpd

Port: 20-21

Configuration File: /etc/vsftpd/vsftpd.conf

Practical case:

- touch /etc/vsftpd/chroot_list
- systemctl start vsftpd

Test: filezilla

Configuration file

/etc/vsftpd/vsftpd.conf:

```
# Anonymous access  
anonymous_enable=NO  
  
# Local enable  
local_enable=YES  
  
# SSL/TLS  
ssl_enable=NO  
  
# filezilla Compatibility  
ssl_ciphers=HIGH  
require_ssl_reuse=NO
```

SENDMAIL

Aim: Transfer emails in a secure way among hosts using SMTP protocol

Install: yum -y install sendmail sendmail-cf m4 cyrus-sasl cyrus-sasl-plain

Port: 25

Configuration file: /etc/mail/sendmail.mc

Previous configuration:

- alternatives --config mta
- systemctl stop postfix

Practical case:

- newaliases
- systemctl start saslauthd
- systemctl start sendmail

Test: echo `date` | mail to user@domain

SENDMAIL Certificates

SSL/TSL Certificates:

```
openssl req -sha256 -new -x509 -nodes -newkey rsa:4096 -days 1825 -out  
/etc/pki/tls/certs/sendmail.pem -keyout /etc/pki/tls/certs/sendmail.pem
```

```
openssl x509 -subject -fingerprint -noout -in /etc/pki/tls/certs/sendmail.pem
```

/etc/sysconfig/saslauthd

- FLAGS=-r

/etc/mail/local-host-names

- domain.com

/etc/mail/access

- Connect:192.168.2.0/24 RELAY

/etc/aliases

- root: marc

SENDMAIL

/etc/mail/sendmail.mc

```
define(`confAUTH_OPTIONS', `A p')dnl
TRUST_AUTH_MECH(`EXTERNAL LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL LOGIN PLAIN')dnl
define(`confCACERT_PATH', `/etc/pki/tls/certs')dnl
define(`confCACERT', `/etc/pki/tls/certs/ca-bundle.crt')dnl
define(`confSERVER_CERT', `/etc/pki/tls/certs/sendmail.pem')dnl
define(`confSERVER_KEY', `/etc/pki/tls/certs/sendmail.pem')dnl
DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl
LOCAL_DOMAIN(`localhost.localdomain')dnl
MASQUERADE_AS(`asorc.net')dnl
```

Print Service: CUPS

Aim: Allow system to be a print server. It accepts task from clients, process them and send to the proper print media

Install: yum -y install cups cups-pdf

Port: 631

Configuration file: /etc/cups/cupsd.conf

Practical case:

- Print in pdf mode: *.pdf
- systemctl start cups

Web admin: <http://localhost:631>

CUPS configuration file

/etc/cups/cupsd.conf:

```
Listen localhost:631 Port 631  
Browsing On  
BrowseOrder allow,deny  
BrowseAllow all  
BrowseRemoteProtocols CUPS  
BrowseAddress @LOCAL  
BrowseLocalProtocols CUPS dnssd  
<Location />  
    Order allow,deny  
    Allow all  
</Location>
```

/etc/cups/cups-pdf.conf

```
Out ${HOME}
```

Servidor LDAP

Objetivo: Permite el acceso a un servicio de directorio ordenado y distribuido para buscar información en un entorno de red. Se puede considerar una base de datos.

Instalación: yum -y install openldap-clients openldap-servers authconfig authconfig-gtk migrationtools

Puerto: 389

Fichero: /etc/openldap/slapd.conf

Comprobación:

- systemctl start slapd
- ldapsearch -x -b 'uid=marc,ou=People,dc=net,dc=dominio'

Fichero de configuración

Creación de la autoridad certificadora:

```
cd /etc/openldap/cacerts
```

```
echo "01" > ca.srl
```

```
openssl genrsa -aes128 2048 > cacert.key
```

```
openssl req -utf8 -new -key cacert.key -out cacert.csr
```

```
openssl x509 -req -in cacert.csr -out cacert.pem -signkey  
cacert.key -days 3650
```

Certificado y firma digital para el servidor:

```
openssl genrsa -aes128 2048 > key.pem
```

```
openssl req -utf8 -new -key key.pem -out slapd.csr
```

Fichero de configuración

/etc/sysconfig/ldap

SLAPD_LDAPS=yes

Configuración:

cp /usr/share/openldap-servers/DB_CONFIG.example
/var/lib/ldap/autenticar/DB_CONFIG

slappasswd (copiar salida)

/etc/openldap/slapd.conf

rootpw (copiar la salida de slappasswd)

Fichero de configuración

Configuración de la seguridad:

```
cacertdir_rehash /etc/openldap/cacerts
```

```
chown -R root:ldap /etc/openldap/cacerts
```

```
chmod -R 750 /etc/openldap/cacerts
```

```
chown -R ldap:ldap /var/lib/ldap/autenticar
```

```
chmod 700 /var/lib/ldap/autenticar
```

```
chown ldap:ldap /etc/openldap/slapd.conf
```

```
chmod 600 /etc/openldap/slapd.conf
```

```
rm -rf /etc/openldap/slapd.d/*
```

Fichero de configuración

Insertar datos en el directorio:

Crea archivos standard

```
echo "" | slapadd -f /etc/openldap/slapd.conf
```

Crear subconjunto de archivos ldif

```
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/
```

Configuración para la migración de cuentas

/usr/share/migrationtools/migrate_common.ph

```
$DEFAULT_MAIL_DOMAIN = "domain.net";
```

```
$DEFAULT_BASE = "dc=domain,dc=net"
```

Fichero de configuración

Insertar datos en el directorio:

Crea el objeto base

```
/usr/share/migrationtools/migrate_base.pl > base.ldif
```

Importar usuarios y grupos

```
/usr/share/migrationtools/migrate_group.pl /etc/group > group.ldif
```

```
/usr/share/migrationtools/migrate_passwd.pl /etc/passwd > passwd.ldif
```

Insertar todo en LDAP

```
ldapadd -x -W -D 'cn=Manager,dc=domino,dc=net' -h 127.0.0.1 -f base.ldif
```

```
ldapadd -x -W -D 'cn=Manager,dc=dominio,dc=net' -h 127.0.0.1 -f group.ldif
```

```
ldapadd -x -W -D 'cn=Manager,dc=dominio,dc=net' -h 127.0.0.1 -f  
passwd.ldif
```

Servidor MYSQL

Objetivo: Gestionar un sistema de bases de datos.

Instalación: yum -y install mariadb mariadb-server

Puerto: 3306

Caso práctico:

- systemctl start mariadb
- mysql_secure_instalation
- mysql -u root -p
 - create database music
 - grant all on music.* to 'marc'@'%' identified by 'passwd'

Comprobación:

Servidor HTTP

Objetivo: Servir contenido web

Instalación: yum -y install httpd

Puerto: 80

Fichero: /etc/httpd/conf.d/*.conf

Caso práctico:

- systemctl start httpd
- Incluir nombre de dominio en el DNS (opcional)

Comprobación:

- http://192.168.2.2
- http://www.embutidosgutierrez.com

Fichero de configuración

/etc/httpd/conf/httpd.conf

 ServerName www.myserver.name:80

/etc/httpd/conf.d/embutidosgutierrez.conf

<VirtualHost *:80>

 DocumentRoot /var/www/html/embutidosgutierrez

 ServerName www.embutidosgutierrez.net

</VirtualHost>

/var/www/html/embutidosgutierrez/index.html

<html>

 <head></head>

 <body> Web de Embutidos Gutierrez </body>

</html>

Fichero de configuración

/etc/named.conf

```
zone "embutidosgutierrez.com" in {  
    type master;  
    file "embutidos.zone";  
}
```

/var/named/embutidos.zone

\$TTL 86400

@ IN SOA network.net root.network.net.

(150115 28800 7200 604800 86400)

IN NS servidor.network.net.

IN MX 10 servidor.network.net.

www.embutidosgutierrez.com. IN A 192.168.2.100

Servidor VPN

Objetivo: Crear una conexión segura entre dos red a través de Internet. Todo el tráfico que viaja está asegurado y protegido.

Instalación: yum -y install openvpn easy-rsa openssl

Puerto: 1194

Fichero:

- Servidor: /etc/openvpn/servidor.conf
- Cliente: /etc/openvpn/cliente.conf

Caso práctico:

- Creación de la red VPN 192.168.37.0
- systemctl --config servidor.conf

Comprobación:

- ifconfig
- ping 192.168.37.1

Servidor VPN

Configuración previa:

- cp -r /usr/share/easy-rsa/2.0/* /etc/openvpn

Creación de certificados:

- mkdir /etc/openvpn/keys/
- /usr/share/easy-rsa/2.0/build-ca
- /usr/share/easy-rsa/2.0/build-dh
- /usr/share/easy-rsa/2.0/build-key-server servidor
- /usr/share/easy-rsa/2.0/build-key cliente

Servidor VPN

/etc/openvpn/servidor.conf

```
port 1194
proto udp
dev tun
### Sección de firma y certificados
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/servidor.crt
key /etc/openvpn/keys/servidor.key
dh keys/dh2048.pem
###
persserver 192.168.37.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
ist-key
persist-tun
status status-openvpn.log
```

Servidor VPN

/etc/openvpn/cliente.conf

client

dev tun

proto udp

remote 192.168.2.2 1194

float

resolv-retry infinite

nobind

persist-key

persist-tun

Sección de firma y certificados

Servidor JABBER

Objetivo: (XMPP) Protocolo extensible de mensajería y comunicación de presencia basado en XML, originalmente ideado para mensajería instantánea.

Instalación:

- Necesario Java (JRE), Mysql
- Openfire:

<http://www.igniterealtime.org/downloads/index.jsp#openfire>

- systemctl start openfire

Configuración web: <http://192.168.2.2:9090>

Comprobación: pidgin

Fichero de configuración

/etc/sysconfig/openfire

- OPENFIRE_OPTS="-Xmx1024m"
- JAVA_HOME=/usr/java/latest

mysql -u root -p

```
create database openfire;  
create user openfire identified by 'passwd';  
grant all on openfire.* to 'openfire'@'%';
```

Servidor ZIMBRA

Objetivo: Programa informático colaborativo con un cliente/servidor de correo, calendario, etc...

Instalación:

http://files2.zimbra.com/downloads/8.5.0_GA/zcs-8.5.0_GA_3042.RHEL6_64.20140828192005.tgz

Caso práctico:

- tar zxvf zcs-8.5.0_GA_3042.RHEL6_64.20140828192005.tgz
- cd zcs-8.5.0_GA_3042.RHEL6_64.20140828192005
- ./install.sh
- service start zimbra

Comprobación: <https://192.168.2.2:7071>

Servidor NAGIOS

Objetivo: Monitor de red que vigila equipos (hardware) y servicios (software) definidos, alertando cuando su comportamiento no es el deseado.

Instalación: yum -y install nagios nagios-plugins-all

Fichero: /etc/httpd/conf.d/nagios.conf

Caso práctico:

- htpasswd /etc/nagios/passwd nagiosadmin
- systemctl start nagios

Comprobación: <http://192.168.2.2/nagios>

Fichero de configuración

/etc/httpd/conf.d/nagios

```
<IfModule !mod_authz_core.c>
# Order allow,deny
# Allow from all
Order deny,allow
Deny from all
Allow from 127.0.0.1 192.168.2.0/24
```

Servidor SQUID

Objetivo: Mejorar el rendimiento de las conexiones web guardando en caché peticiones recurrentes, acelerar el acceso al servidor web y añadir seguridad filtrando tráfico.

Instalación: yum -y install squid

Puerto: 3128

Fichero: /etc/squid/squid.conf

Caso práctico:

- redirección del tráfico (script: /etc/squid/redirect.sh)
- systemctl start squid

Comprobación: <http://www.elpais.es>

Fichero de configuración

/etc/squid/squid.conf

- acl network src 192.168.2.0/24
- acl web_deny url_regex "/etc/squid/web_deny.acl"
- http_access allow list_deny !web_deny
- http_port 3128

/etc/squid/web-deny.acl

- www.elpais.es

Fichero de configuración

Redirección del tráfico hacia el proxy-cache (scripting):

- Interfaz enp0s3: WAN
- Interfaz enp0s8: LAN

/etc/squid/redirect.sh

Permite el paso de una red a la otra

```
iptables -A FORWARD -i enp0s8 -o enp0s3 -j  
ACCEPT
```

Envío del tráfico entrante por enp0s8 hacia el proxy

```
iptables -t nat -A PREROUTING -i enp0s8 -p tcp -m  
tcp --dport 80 -j DNAT --to-destination  
192.168.2.2:3128
```

Envío del tráfico saliente a la red externa

Servidor LTSP

Objetivo: Proporcionar la capacidad de ejecutar Linux en computadores de pocas prestaciones. El sistema consiste en distribuir a los clientes, por medio de la red, el núcleo Linux que se está ejecutando en el servidor.

Previo:

Obtener un thin-client: <http://distrowatch.com/>

Volcar la distro en /opt/ltsp/amd64

Instalación: yum -y install nfs-utils dhcpcd tftp-server syslinux

Fichero de configuración

Configuración:

```
cp -r /usr/share/syslinux/* /var/lib/tftpboot/
```

```
mkdir /var/lib/tftpboot/pxelinux.cfg;
```

/etc(exports

```
 /opt/ltsp/amd64 *(ro,async,no_root_squash)
```

/etc/dhcpd/dhcpd.conf

```
class "pxeclients" {
```

```
match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
```

```
next-server 192.168.2.2;
```

```
filename "pxelinux.0";
```

```
option root-path "192.168.2.2:/opt/ltsp/amd64";
```

```
}
```

Fichero de configuración

/etc/xinetd.d/tftp

service tftp

{

socket_type = dgram

protocol = udp

wait = yes

user = root

server = /usr/sbin/in.tftpd

server_args = -s /var/lib/tftpboot

disable = no

per_source = 11

Fichero de configuración

Caso práctico:

systemctl restart nfs-server

systemctl restart dhcpd

systemctl restart xinetd

Comprobación:

Arrancar el cliente con la opción “Arranque por red”.

Servidor PXE

Objetivo: Crear un entorno para arrancar e instalar el sistema operativo en computadoras a través de una red.

Instalación: yum -y install dhcpcd tftp-server vsftpd syslinux

Configuración previa:

- mount -t iso9660 -o loop CentOS-7-x86_64-Minimal.iso /var/ftp
- cp /var/ftp/images/pxeboot/vmlinuz /var/lib/tftpboot/centos/
- cp /var/ftp/images/pxeboot/initrd.img /var/lib/tftpboot/centos/
- cp -r /usr/share/syslinux/* /var/lib/tftpboot/
- mkdir /var/lib/tftpboot/pxelinux.cfg

Fichero de configuración

/var/lib/tftpboot/pxelinux.cfg/default

```
default menu.c32
```

```
prompt 0
```

```
timeout 300
```

```
ONTIMEOUT local
```

```
menu title ##### PXE Boot Menu #####
```

```
label 1
```

```
menu label ^1) Install Centos 7-Minimal 64-bit
```

```
kernel centos/vmlinuz
```

```
append initrd=centos/initrd.img method=ftp://192.168.2.2/centos devfs=nomount
```

Fichero de configuración

Servicio FTP /etc/vsftpd/vsftpd.conf

anonymous_enable=YES

no_anon_password=YES

anon_root=/var/ftp/

anon_upload_enable=NO

anon_mkdir_write_enable=NO

Servicio dhcpcd:

- Igual que para LTSP

Servicio tftp:

- Igual que para LTSP

Fichero de configuración

Caso práctico:

- systemctl restart vsftpd
- systemctl restart dhcpd
- systemctl restart xinetd

Comprobación:

Arrancar el cliente con la opción “Arranque por red”.

Servidor DRBL

Objetivo: Permite tener un S.O. corriendo en varias máquinas sin necesidad de que tengan un disco duro conectado.

También permite clonar o restaurar varios equipos a la vez mediante paquetes Multicast.

Instalación: No requiere instalación.

Caso práctico:

- <http://drbl.org/download>

Comprobación:

- Arrancar el servidor.
- Arrancar el cliente con la opción “Arranque por red”.

RAID

Objetivo: Permite implementar un volumen de almacenamiento de datos formado por varios discos duros con el objetivo de proteger la información y conseguir mayor tolerancia a fallos si el disco duro sufre una avería.

Instalación: yum -y install mdadm

Caso práctico:

Creación del raid con cuatro discos duros:

```
mdadm --create /dev/md1 --level=raid10 --raid-device=4 /dev/sdb /dev/sdc /dev/sdd  
/dev/sde
```

Configuración:

```
mdadm --detail --scan >> /etc/mdadm.conf
```

Simular fallo de disco: mdadm -f /dev/md1 /dev/sdb

Extraer disco del RAID: mdadm -r /dev/md1 /dev/sdb

Añadir disco al RAID: mdadm -a /dev/md1 /dev/sdb

Comprobación: mdadm --detail /dev/md1

RAID

Objetivo: Creación de un volumen lógico. Configurar el RAID para usarlo como un directorio del sistema de ficheros.

```
pvcreate /dev/md1
```

```
vgcreate VGDatos /dev/md1
```

```
lvcreate -l 90%FREE VGDatos -n LVDatos
```

```
mkfs.ext4 /dev/mapper/VGDatos-LVDatos
```

```
mkdir -p /datos
```

```
mount /dev/mapper/VGDatos /datos
```

IPTABLES

Objetivo: Es un firewall integrado en el kernel. Permite interceptar y manipular paquetes que circulan por la red.

Instalación: yum -y install iptables

Caso práctico:

- Entrada por interfaz enp3s0 (LAN 192.168.2.0/24)
- Salida por interfaz enp4s0 (WAN internet)

Comprobación:

- iptables -L -n --lines-numbers
- iptables -L -n --lines-numbers -t nat

Fichero de configuración

/root/iptables.sh (scripting)

Eliminar reglas anteriores

iptables -F; iptables -X

iptables -Z; iptables -t nat -F

Establecer politicas por defecto

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

Paso de paquetes entre interfaces

iptables -A FORWARD -i enp3s0 -o enp4s0 -s
192.168.2.0/24 -m conntrack --ctstate NEW -j
ACCEPT

Servidor NIS

Objetivo: Permitir el envío de datos de configuración tales como nombres de usuarios y hosts dentro de una red.

Instalación: yum -y install ypbind yp-tools ypserv

Caso práctico:

- domainname ypdomain.net
- systemctl start ypserv

Comprobación: rpcinfo -u localhost ypserv

Fichero de configuración

Fichero:

/etc/yp.conf

- domain ypdomain.net server 192.168.2.2

/etc/hosts

- 192.168.2.2 server

/etc/yp.serv.conf

- dns: no
- files: 30
- xfr_check_port: yes
- *: *: shadow.byname: port
- *: *: password.adjunct.byname: port

/etc/svsconfig/network