## Infraestructura Necesaria:

→ **kb-servidor.ejemplo.com** ==> **192.168.100.150/24** **(CentOS-7.x)**
→ **kb-cliente.ejemplo.com** ==> **192.168.100.151/24** **(CentOS-7.x)**

## 1 ==> CONFIGURACIÓN -NFS- CARA 'SERVIDOR' → *kb-servidor.ejemplo.com*

```
# yum install nfs-utils
# firewall-cmd --permanent --add-service=nfs
# firewall-cmd --reload

# mkdir /var/nfs
# chmod 0777 /var/nfs
->#  chown nobody:nobody /mnt/nfs
```

→ *Editamos '**/etc/idmap.conf**' de la forma:*

```
->      [Mapping]

        Nobody-User = nobody
        Nobody-Group = nobody

# systemctl enable rpcbind nfs-server
# systemctl start rpcbind nfs-server
# systemctl status rpcbind nfs-server
# cat /etc/services |grep 2049
        nfs         2049/tcp        nfsd shilp      # Network File System
        nfs         2049/udp        nfsd shilp      # Network File System
        nfs         2049/sctp       nfsd shilp      # Network File System
```

→ *Editamos '**/etc/exports**' de la forma:*

```
        /var/nfs      kb-cliente.ejemplo.com(rw,no_root_squash)
```

*(Si se utiliza **no_root_squash**, los usuarios root remotos tienen la posibilidad de modificar cualquier archivo en el sistema de archivos compartido, y dejar aplicaciones infectadas con troyanos para que otros usuarios las ejecuten sin saberlo).*

```
# systemctl restart nfs-server rpcbind

# exportfs -avr
        exporting kb-cliente.ejemplo.com:/var/nfs

# showmount -e localhost
        Export list for localhost:
        /var/nfs kb-cliente.ejemplo.com
```

*# cat /var/lib/nfs/etab*
*/var/nfs kb-cliente.ejemplo.com(rw,sync,wdelay,hide,nocrossmnt,secure,no_root_squash,no_all_squash,no_subtree_check,secure_locks,acl,no_pnfs,**anonuid=65534,anongid=65534**,sec=sys,rw,secure,no_root_squash,no_all_squash)*

***2 ==> CONFIGURACIÓN -NFS- CARA 'CLIENTE' → kb-cliente.ejemplo.com***

*# yum install nfs-utils*

*# systemctl enable rpcbind*
*# systemctl start rpcbind*
*# systemctl status rpcbind*

*# mkdir /mnt/nfs*
*# chmod 0777 /mnt/nfs*
*->*# chown nobody:nobody /mnt/nfs*

→ *Editamos '**/etc/idmap.conf**' de la forma:*

-> *[Mapping]*

*Nobody-User = nobody*
*Nobody-Group = nobody*

→ *Editamos '**/etc/fstab**' de la forma:*

***kb-servidor.ejemplo.com:/var/nfs /mnt/nfs nfs _netdev,rw 0 0***

→ *Montaje (una de las dos formas):*

*# mount -a*
*# mount -t nfs -o rw kb-servidor:/var/nfs /mnt/nfs*

→ *Comprobaciones:*

*[root@kb-servidor carlos]# touch /var/nfs/fichero_servidor.txt*
*[root@kb-cliente carlos]# touch /mnt/nfs/fichero_cliente.txt*

*[root@kb-servidor carlos]# ls /var/nfs/*
*fichero_cliente.txt fichero_servidor.txt*

*[root@kb-cliente carlos]# ls /mnt/nfs/*
*fichero_cliente.txt fichero_servidor.txt*

→ *Monitorización:*

```
[root@kb-servidor carlos]# nfsstat
Server rpc stats:
calls      badcalls   badclnt    badauth    xdrcall
121        0          0          0          0

Server nfs v4:
null         compound
3         2% 118      97%

Server nfs v4 operations:
op0-unused   op1-unused   op2-future   access       close        commit
0         0% 0         0% 0         0% 12        4% 1         0% 0         0%
create       delegpurge   delegreturn  getattr      getfh        link
0         0% 0         0% 0         0% 83        33% 16       6% 0         0%
lock         lockt        locku        lookup       lookup_root  nverify
0         0% 0         0% 0         0% 11        4% 0         0% 0         0%
open         openattr     open_conf    open_dgrd    putfh        putpubfh
1         0% 0         0% 1         0% 0         0% 82        33% 0        0%
putrootfh    read         readdir      readlink     remove       rename
4         1% 0         0% 2         0% 0         0% 0         0% 0         0%
renew        restorefh    savefh       secinfo      setattr      setcltid
24        9% 0         0% 0         0% 0         0% 1         0% 4         1%
setcltidconf verify       write        rellockowner bc_ctl       bind_conn
4         1% 0         0% 0         0% 0         0% 0         0% 0         0%
exchange_id  create_ses   destroy_ses  free_stateid getdirdeleg  getdevinfo
0         0% 0         0% 0         0% 0         0% 0         0% 0         0%
getdevlist   layoutcommit layoutget    layoutreturn secinfononam sequence
0         0% 0         0% 0         0% 0         0% 0         0% 0         0%
set_ssv      test_stateid want_deleg   destroy_clid reclaim_comp
0         0% 0         0% 0         0% 0         0% 0         0%

[root@kb-cliente carlos]# nfsstat
Server rpc stats:
calls      badcalls   badclnt    badauth    xdrcall
0          0          0          0          0

Client rpc stats:
calls      retrans    authrefrsh
143        0          143

Client nfs v4:
null         read         write        commit       open         open_conf
0         0% 0         0% 0         0% 0         0% 1         0% 1         0%
open_noat    open_dgrd    close        setattr      fsinfo       renew
0         0% 0         0% 1         0% 1         0% 12        8% 25        18%
setclntid    confirm      lock         lockt        locku        access
10        7% 4         2% 0         0% 0         0% 0         0% 11        8%
```

```
getattr    lookup     lookup_root  remove     rename     link
14     10% 11     8% 16     11% 0      0% 0      0% 0      0%
symlink    create     pathconf   statfs     readlink   readdir
0      0% 0      0% 8      5% 0      0% 0      0% 2      1%
server_caps  delegreturn  getacl     setacl     fs_locations rel_lkowner
20     14% 0      0% 0      0% 0      0% 0      0% 0      0%
secinfo    exchange_id  create_ses   destroy_ses  sequence   get_lease_t
0      0% 0      0% 0      0% 0      0% 0      0% 0      0%
reclaim_comp layoutget   getdevinfo   layoutcommit layoutreturn getdevlist
0      0% 0      0% 0      0% 0      0% 0      0% 0      0%
(null)
0      0%
```

```
[root@kb-cliente carlos]# nfsiostat

kb-servidor:/var/nfs mounted on /mnt/nfs:

   op/s         rpc bklog
   0.08    0.00
read:          ops/s            kB/s           kB/op         retrans      avg RTT (ms)  avg exe
(ms)
                 0.000   0.000   0.000      0 (0.0%)     0.000   0.000
write:         ops/s            kB/s           kB/op         retrans      avg RTT (ms)  avg exe
(ms)
                 0.000   0.000   0.000      0 (0.0%)     0.000   0.000

[root@kb-cliente carlos]# mountstats /mnt/nfs/
Stats for kb-servidor:/var/nfs mounted on /mnt/nfs:
  NFS mount options:
rw,vers=4.0,rsize=131072,wsize=131072,namlen=255,acregmin=3,acregmax=60,acdirmin=30,ac
dirmax=60,hard,proto=tcp,port=0,timeo=600,retrans=2,sec=sys,clientaddr=192.168.100.151,loc
al_lock=none
  NFS server capabilities: caps=0xffdf,wtmult=512,dtsize=32768,bsize=0,namlen=255
  NFSv4 capability flags: bm0=0xfdffbfff,bm1=0xf9be3e,bm2=0x0,acl=0x3,pnfs=notconfigured
  NFS security flavor: 1  pseudoflavor: 0

NFS byte counts:
  applications read 0 bytes via read(2)
  applications wrote 0 bytes via write(2)
  applications read 0 bytes via O_DIRECT read(2)
  applications wrote 0 bytes via O_DIRECT write(2)
  client read 0 bytes via NFS READ
  client wrote 0 bytes via NFS WRITE

RPC statistics:
  49 RPC requests sent, 49 RPC replies received (0 XIDs not found)
```

*average backlog queue length: 0*

*GETATTR:*
*7 ops (14%)*
*avg bytes sent per op: 156 avg bytes received per op: 196*
*backlog wait: 0.000000 RTT: 0.857143 total execute time: 0.857143 (milliseconds)*
*ACCESS:*
*4 ops (8%)*
*avg bytes sent per op: 164 avg bytes received per op: 124*
*backlog wait: 0.000000 RTT: 0.750000 total execute time: 0.750000 (milliseconds)*
*READDIR:*
*2 ops (4%)*
*avg bytes sent per op: 180 avg bytes received per op: 296*
*backlog wait: 0.000000 RTT: 0.500000 total execute time: 0.500000 (milliseconds)*
*SERVER_CAPS:*
*2 ops (4%)*
*avg bytes sent per op: 152 avg bytes received per op: 92*
*backlog wait: 0.000000 RTT: 0.500000 total execute time: 0.500000 (milliseconds)*
*OPEN:*
*1 ops (2%)*
*avg bytes sent per op: 276 avg bytes received per op: 328*
*backlog wait: 0.000000 RTT: 7.000000 total execute time: 7.000000 (milliseconds)*
*OPEN_CONFIRM:*
*1 ops (2%)*
*avg bytes sent per op: 176 avg bytes received per op: 68*
*backlog wait: 0.000000 RTT: 133.000000 total execute time: 133.000000 (milliseconds)*
*CLOSE:*
*1 ops (2%)*
*avg bytes sent per op: 192 avg bytes received per op: 132*
*backlog wait: 0.000000 RTT: 0.000000 total execute time: 0.000000 (milliseconds)*
*SETATTR:*
*1 ops (2%)*
*avg bytes sent per op: 212 avg bytes received per op: 220*
*backlog wait: 0.000000 RTT: 3.000000 total execute time: 3.000000 (milliseconds)*
*FSINFO:*
*1 ops (2%)*
*avg bytes sent per op: 156 avg bytes received per op: 108*
*backlog wait: 0.000000 RTT: 0.000000 total execute time: 0.000000 (milliseconds)*
*LOOKUP:*

*1 ops (2%)*
*avg bytes sent per op: 172 avg bytes received per op: 244*
*backlog wait: 0.000000 RTT: 0.000000 total execute time: 0.000000 (milliseconds)*
*PATHCONF:*
*1 ops (2%)*
*avg bytes sent per op: 152 avg bytes received per op: 72*
*backlog wait: 0.000000 RTT: 0.000000 total execute time: 0.000000 (milliseconds)*

*[root@kb-cliente carlos]# mount |grep /var/nfs*
***kb-servidor:/var/nfs on /mnt/nfs type nfs4***
*(rw,relatime,vers=4.0,rsize=131072,wsize=131072,namlen=255,hard,proto=tcp,port=0,timeo=600,retrans=2,sec=sys,clientaddr=192.168.100.151,local_lock=none,addr=192.168.100.150)*

*[root@kb-cliente carlos]# df -h |grep /var/nfs*
*kb-servidor:/var/nfs 18G 1,4G 17G 8% /mnt/nfs*

## *3 ==> SEGURIDAD kerberos en -NFS- CARA 'SERVIDOR' → kb-servidor.ejemplo.com*

→ *Visualizamos los '**keytab**':*

*[root@kb-servidor carlos]# **ktutil***
***ktutil: read_kt /etc/krb5.keytab***
*ktutil: **l***
*slot KVNO Principal*
*---- ---- ---------------------------------------------------------------------*
*1 9 host/kb-servidor.ejemplo.com@EJEMPLO.COM*
*2 9 host/kb-servidor.ejemplo.com@EJEMPLO.COM*
*3 9 host/kb-servidor.ejemplo.com@EJEMPLO.COM*
*4 9 host/kb-servidor.ejemplo.com@EJEMPLO.COM*
*5 9 host/kb-servidor.ejemplo.com@EJEMPLO.COM*
*6 9 host/kb-servidor.ejemplo.com@EJEMPLO.COM*
*7 9 host/kb-servidor.ejemplo.com@EJEMPLO.COM*
*8 9 host/kb-servidor.ejemplo.com@EJEMPLO.COM*
*9 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM*
*10 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM*
*11 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM*
*12 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM*
*13 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM*
*14 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM*
*15 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM*
*16 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM*
*ktutil: **q***

→ *Editamos '**/etc/exports**' de la forma:*

*/var/nfs kb-cliente.ejemplo.com(**sec=krb5p**,rw,no_root_squash)*

```
[root@kb-servidor carlos]# exportfs -avr
exporting kb-cliente.ejemplo.com:/var/nfs

[root@kb-servidor carlos]# showmount -e
Export list for kb-servidor.ejemplo.com:
/var/nfs kb-cliente.ejemplo.com
```

→ *Activamos Protección (ver: '**man exports**' → **krb5p)**.*

```
# systemctl enable nfs-secure-server
# systemctl start nfs-secure-server
# systemctl status nfs-secure.service
● rpc-gssd.service - RPC security service for NFS client and server
Loaded: loaded (/usr/lib/systemd/system/rpc-gssd.service; static; vendor preset: disabled)
Active: active (running) since mar 2017-02-14 06:36:22 CET; 2h 47min ago
Main PID: 661 (rpc.gssd)
CGroup: /system.slice/rpc-gssd.service
└─661 /usr/sbin/rpc.gssd

feb 14 06:36:22 kb-servidor.ejemplo.com systemd[1]: Starting RPC security service for NFS client and server...
feb 14 06:36:22 kb-servidor.ejemplo.com systemd[1]: Started RPC security service for NFS client and server.
```

→ *Aumentar verbosidad en '**/var/log/messages**' modificando las variables siguientes en '**/etc/sysconfig/nfs**' de la forma:*

```
RPCIDMAPDARGS="-vvv"
RPCSVCGSSDARGS="-vvv"
```

```
# systemctl restart nfs-secure-server nfs-idmap rpcbind
# systemctl status nfs-secure-server nfs-idmap rpcbind
● rpc-gssd.service - RPC security service for NFS client and server
  Loaded: loaded (/usr/lib/systemd/system/rpc-gssd.service; static; vendor preset: disabled)
  Active: active (running) since mar 2017-02-14 20:09:24 CET; 20s ago
 Process: 3026 ExecStart=/usr/sbin/rpc.gssd $GSSDARGS (code=exited, status=0/SUCCESS)
Main PID: 3028 (rpc.gssd)
  CGroup: /system.slice/rpc-gssd.service
          └─3028 /usr/sbin/rpc.gssd

feb 14 20:09:24 kb-servidor.ejemplo.com systemd[1]: Starting RPC security service for NFS client and server...
feb 14 20:09:24 kb-servidor.ejemplo.com systemd[1]: Started RPC security service for NFS client and server.

● rpcbind.service - RPC bind service
  Loaded: loaded (/usr/lib/systemd/system/rpcbind.service; indirect; vendor preset: enabled)
  Active: active (running) since mar 2017-02-14 20:09:24 CET; 20s ago
 Process: 3023 ExecStart=/sbin/rpcbind -w $RPCBIND_ARGS (code=exited, status=0/SUCCESS)
```

```
Main PID: 3025 (rpcbind)
  CGroup: /system.slice/rpcbind.service
          └─3025 /sbin/rpcbind -w

feb 14 20:09:24 kb-servidor.ejemplo.com systemd[1]: Starting RPC bind service...
feb 14 20:09:24 kb-servidor.ejemplo.com systemd[1]: Started RPC bind service.

[root@kb-servidor carlos]# tail -f /var/log/messages
Feb 14 09:01:01 kb-servidor systemd: Starting user-0.slice.
Feb 14 09:01:01 kb-servidor systemd: Started Session 4 of user root.
Feb 14 09:01:01 kb-servidor systemd: Starting Session 4 of user root.
Feb 14 09:01:01 kb-servidor systemd: Removed slice user-0.slice.
Feb 14 09:01:01 kb-servidor systemd: Stopping user-0.slice.
Feb 14 09:33:48 kb-servidor systemd: Stopping RPC security service for NFS client and server...
Feb 14 09:33:48 kb-servidor systemd: Starting Preprocess NFS configuration...
Feb 14 09:33:48 kb-servidor systemd: Started Preprocess NFS configuration.
Feb 14 09:33:48 kb-servidor systemd: Starting RPC security service for NFS client and server...
Feb 14 09:33:48 kb-servidor systemd: Started RPC security service for NFS client and server.
```

## 4 ==> SEGURIDAD kerberos en -NFS- CARA 'CLIENTE' → kb-cliente.ejemplo.com

→ *Visualizamos los '**keytab**':*

```
[root@kb-cliente carlos]# ktutil
ktutil:  read_kt /etc/krb5.keytab
ktutil:  l
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
1    9 host/kb-servidor.ejemplo.com@EJEMPLO.COM
2    9 host/kb-servidor.ejemplo.com@EJEMPLO.COM
3    9 host/kb-servidor.ejemplo.com@EJEMPLO.COM
4    9 host/kb-servidor.ejemplo.com@EJEMPLO.COM
5    9 host/kb-servidor.ejemplo.com@EJEMPLO.COM
6    9 host/kb-servidor.ejemplo.com@EJEMPLO.COM
7    9 host/kb-servidor.ejemplo.com@EJEMPLO.COM
8    9 host/kb-servidor.ejemplo.com@EJEMPLO.COM
9    8  host/kb-cliente.ejemplo.com@EJEMPLO.COM
10   8  host/kb-cliente.ejemplo.com@EJEMPLO.COM
11   8  host/kb-cliente.ejemplo.com@EJEMPLO.COM
12   8  host/kb-cliente.ejemplo.com@EJEMPLO.COM
13   8  host/kb-cliente.ejemplo.com@EJEMPLO.COM
14   8  host/kb-cliente.ejemplo.com@EJEMPLO.COM
15   8  host/kb-cliente.ejemplo.com@EJEMPLO.COM
16   8  host/kb-cliente.ejemplo.com@EJEMPLO.COM
ktutil:  q
```

→ *Modificar '**/etc/fstab**' de la forma:*

*kb-servidor.ejemplo.com:/var/nfs /mnt/nfs nfs* ***sec=krb5p*** *0 0*

```
[root@kb-cliente carlos]# systemctl enable nfs-secure
[root@kb-cliente carlos]# systemctl start nfs-secure
[root@kb-cliente carlos]# systemctl status nfs-secure
● rpc-gssd.service - RPC security service for NFS client and server
   Loaded: loaded (/usr/lib/systemd/system/rpc-gssd.service; static; vendor preset: disabled)
   Active: active (running) since mar 2017-02-14 20:33:34 CET; 6s ago
  Process: 3193 ExecStart=/usr/sbin/rpc.gssd $GSSDARGS (code=exited, status=0/SUCCESS)
 Main PID: 3194 (rpc.gssd)
   CGroup: /system.slice/rpc-gssd.service
           └─3194 /usr/sbin/rpc.gssd

feb 14 20:33:34 kb-cliente.ejemplo.com systemd[1]: Starting RPC security service for NFS client and server...
feb 14 20:33:34 kb-cliente.ejemplo.com systemd[1]: Started RPC security service for NFS client and server.
```

→ *Aumentar verbosidad en '**/var/log/messages**' modificando las variables siguientes en '**/etc/sysconfig/nfs**' de la forma:*

***RPCIDMAPDARGS="-vvv"***
***RPCSVCGSSDARGS="-vvv"***

```
[root@kb-cliente carlos]# systemctl restart nfs-idmap nfs-secure

[root@kb-cliente carlos]# systemctl enable nfs-client.target && systemctl start nfs-client.target
```

***BIBLIOGRAFIA:***

** *RHCSA & RHCE RedHat Enterprise Linux 7 – Asghar Ghori.*
** *https://www.certdepot.net/rhel7-use-kerberos-control-access-nfs-network-shares/*