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 CARA 'SERVIDOR' → *kb-servidor.ejemplo.com*

→ Sincronización del Servidor via NTP (mejor chrony/chronyd daemon).

→ Comprobamos ajustes horarios:

```
# timedatectl
Local time: lun 2017-02-06 11:35:21 CET
Universal time: lun 2017-02-06 10:35:21 UTC
RTC time: lun 2017-02-06 10:35:21
Time zone: Europe/Madrid (CET, +0100)
NTP enabled: n/a
NTP synchronized: no
RTC in local TZ: no
DST active: no
Last DST change: DST ended at
dom 2016-10-30 02:59:59 CEST
dom 2016-10-30 02:00:00 CET
Next DST change: DST begins (the clock jumps one hour forward) at
dom 2017-03-26 01:59:59 CET
dom 2017-03-26 03:00:00 CEST
```

→ Instalamos NTP:

```
# yum install ntp -y
# systemctl enable ntpd
# systemctl start ntpd
# systemctl status ntpd
```

→ Configuración en '**/etc/ntp.conf**':

```
…
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst
…
```

→ Información acerca del proceso de sincronización:

```
# ntpq -p
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*ntp.redimadrid. 193.147.107.33   2 u   33   64    3   70.563    0.264   3.187
+213.251.52.234  193.62.22.74     2 u   33   64    3   69.870    0.985   2.341
```

```
#[root@kb-servidor carlos]# ntpstat
unsynchronised
polling server every 64 s
```

→ Detenemos Servicio para poder sincronizar.

```
# systemctl stop ntpd
# ntpdate pool.ntp.org
6 Feb 11:52:33 ntpdate[3358]: adjust time server 158.227.98.15 offset -0.005900 sec
```

→ Iniciamos Servicio de nuevo:

```
# systemctl start ntpd
# ntpstat
synchronised to NTP server (213.251.52.234) at stratum 3
time correct to within 8047 ms
polling server every 64 s
```

→ Instalación de '**chrony**':

```
# yum install chrony
# systemctl enable chronyd
# systemctl start chronyd
# systemctl status chronyd
```

→ Fichero de configuración '**/etc/chrony.conf**'.

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst

# Ignore stratum in source selection.
stratumweight 0
…
```

→ Información acerca de la referencia principal de sincronización:

```
# chronyc tracking
Reference ID    : 158.227.98.15 (i2t15.i2t.ehu.eus)
Stratum         : 2
Ref time (UTC)  : Tue Feb  7 06:31:07 2017
System time     : 0.002491276 seconds slow of NTP time
Last offset     : -0.000464006 seconds
RMS offset      : 0.003813621 seconds
Frequency       : 2.786 ppm slow
Residual freq   : -0.173 ppm
Skew            : 33.491 ppm
Root delay      : 0.075276 seconds
Root dispersion : 0.001305 seconds
Update interval : 64.7 seconds
Leap status     : Normal
```

→ Equivalente a '**ntpq -p**':

```
# chronyc sources -v
210 Number of sources = 4

.-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current synced, '+' = combined , '-' = not combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
||                                               .- xxxx [ yyyy ] +/- zzzz
||     Reachability register (octal) -.          |  xxxx = adjusted offset,
||     Log2(Polling interval) --.      |         |  yyyy = measured offset,
||                               \     |         |  zzzz = estimated error.
||                                |    |         \
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^+ ntp.redimadrid.es             2   6   377    51  +4679us[+4679us] +/-   84ms
^+ 213.251.52.234                2   6   377    52  +2649us[+2649us] +/-   82ms
^+ dnscache-madrid.ntt.eu        2   6   377    50  -6854us[-6854us] +/-  106ms
^* i2t15.i2t.ehu.eus             1   6   377    52  +2812us[+3521us] +/-   41ms

# chronyc sourcestats
210 Number of sources = 4
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
==============================================================================
ntp.redimadrid.es          14  10   654     -0.508     10.829  +4947us  1871us
213.251.52.234             14   7   653     +1.731     10.951  +3935us  2005us
dnscache-madrid.ntt.eu     14   8   654     +6.719     17.338  -7979us  3790us
i2t15.i2t.ehu.eus          14  12   653     -2.928     39.940  -1106us  7298us
```

→ Sincronización rápida (**NO** es necesario parar el servicio → '**chronyd**').

```
# ntpdate pool.ntp.org
```

7 Feb 07:40:20 ntpdate[2591]: adjust time server 158.227.98.15 offset -0.004089 sec

→ Cualificación Completa del Servidor (FQDN).

```
# hostnamectl set-hostname kb-servidor.ejemplo.com
# hostnamectl
        Static hostname: kb-servidor.ejemplo.com
         Icon name: computer-vm
        ...
```

→ Configuraciones: → -**NO-** Configuramos **DNS's** para el ejemplo (red interna):

→ → Contenido '**/etc/hosts**':

```
...
192.168.100.150      kb-servidor.ejemplo.com
192.168.100.151      kb-cliente.ejemplo.com
…
```

→ →Contenido '**/etc/resolv.conf**':

```
# Generated by NetworkManager
search ejemplo.com
nameserver 192.168.100.1
```

→ Paqueteria Necesaria:

```
# yum install krb5-server krb5-workstation -y
```

→ Editamos '**vi /etc/krb5.conf**', de la forma:

```
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = EJEMPLO.COM
default_ccache_name = KEYRING:persistent:%{uid}

[realms]
```

```
EJEMPLO.COM = {
kdc = kb-servidor.ejemplo.com
admin_server = kb-servidor.ejemplo.com
}

[domain_realm]
.ejemplo.com = EJEMPLO.COM
ejemplo.com = EJEMPLO.COM
```

→ Editamos '**/var/kerberos/krb5kdc/kdc.conf**' de la forma:

```
[kdcdefaults]
kdc_ports = 88
kdc_tcp_ports = 88

[realms]
EJEMPLO.COM = {
master_key_type = aes256-cts

# Eliminamos Compatibilidad Kerberos 4 (Mejora en Seguridad).
default_principal_flags = +preauth

acl_file = /var/kerberos/krb5kdc/kadm5.acl
dict_file = /usr/share/dict/words
admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
supported_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal
arcfour-hmac:normal camellia256-cts:normal camellia128-cts:normal des-hmac-
sha1:normal des-cbc-md5:normal des-cbc-crc:normal
}
```

→ Editamos '**/var/kerberos/krb5kdc/kadm5.acl**' de la forma:

```
*/admin@EJEMPLO.COM     *
```

→ Descargamos y compilamos '**haveged**' (Hardware Volatile Entropy Gathering and Expansion), para generar la entropia necesaria.

```
# yum install wget
# wget http://www.issihosts.com/haveged/haveged-1.9.1.tar.gz
# tar xvzf haveged-1.9.1.tar.g
# cd haveged-1.9.1/
# yum install gcc-c++.x86_64
# ./configure
# make && make install

# cat /proc/sys/kernel/random/entropy_avail
131
```

→ Iniciamos daemon:

```
# haveged -w 1024
# cat /proc/sys/kernel/random/entropy_avail
2367
```

→ Procedimiento Alternativo para generar entropia → '**rng-tools'**:

```
# yum install rng-tools
# cat /proc/sys/kernel/random/entropy_avail
160

# rngd -r /dev/urandom
# cat /proc/sys/kernel/random/entropy_avail
2980
```

→ Creamos la database '**principal**' para kerberos:

```
# kdb5_util create -s -r EJEMPLO.COM
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm 'EJEMPLO.COM',
master key name 'K/M@EJEMPLO.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

→ Iniciamos servicios kerberos:

```
# systemctl start krb5kdc kadmin
# systemctl status krb5kdc kadmin
# systemctl enable krb5kdc kadmin
```

→ Creamos '**usuario01**' de prueba.

```
# useradd usuario01
# passwd usuario01
```

→ Ejecutamos herramientas de administración kerberos en modo local:

```
# kadmin.local
Authenticating as principal carlos/admin@EJEMPLO.COM with password.
kadmin.local:  ?
Available kadmin.local requests:

add_principal, addprinc, ank
```

Add principal
delete_principal, delprinc
Delete principal
modify_principal, modprinc
Modify principal
rename_principal, renprinc
Rename principal
change_password, cpw Change password
get_principal, getprinc Get principal
list_principals, listprincs, get_principals, getprincs
List principals
add_policy, addpol Add policy
modify_policy, modpol Modify policy
delete_policy, delpol Delete policy
get_policy, getpol Get policy
list_policies, listpols, get_policies, getpols
List policies
get_privs, getprivs Get privileges
ktadd, xst Add entry(s) to a keytab
ktremove, ktrem Remove entry(s) from a keytab
lock Lock database exclusively (use with extreme caution!)
unlock Release exclusive database lock
purgekeys Purge previously retained old keys from a principal
get_strings, getstrs Show string attributes on a principal
set_string, setstr Set a string attribute on a principal
del_string, delstr Delete a string attribute on a principal
list_requests, lr, ? List available requests.
quit, exit, q Exit program.

→ Creamos '**admin**' principal.

```
#kadmin.local
kadmin.local:  add_principal root/admin
WARNING: no policy specified for root/admin@EJEMPLO.COM; defaulting to no policy
Enter password for principal "root/admin@EJEMPLO.COM":
Re-enter password for principal "root/admin@EJEMPLO.COM":
Principal "root/admin@EJEMPLO.COM" created.
```

→ Creamos el '**usuario01**' principal.

```
kadmin.local:  add_principal usuario01
WARNING: no policy specified for usuario01@EJEMPLO.COM; defaulting to no policy
Enter password for principal "usuario01@EJEMPLO.COM":
Re-enter password for principal "usuario01@EJEMPLO.COM":
Principal "usuario01@EJEMPLO.COM" created.
```

→ Añadimos el KDC hostname a la base de datos kerberos.

```
kadmin.local:  add_principal -randkey host/kb-servidor.ejemplo.com
WARNING: no policy specified for host/kb-servidor.ejemplo.com@EJEMPLO.COM; defaulting to no policy
Principal "host/kb-servidor.ejemplo.com@EJEMPLO.COM" created.
```

→ Creamos una copia local almacenando en '**/etc/krb5.keytab**'

```
kadmin.local:  ktadd host/kb-servidor.ejemplo.com
Entry for principal host/kb-servidor.ejemplo.com with kvno 2, encryption type aes256-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-servidor.ejemplo.com with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-servidor.ejemplo.com with kvno 2, encryption type des3-cbc-sha1 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-servidor.ejemplo.com with kvno 2, encryption type arcfour-hmac added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-servidor.ejemplo.com with kvno 2, encryption type camellia256-cts-cmac added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-servidor.ejemplo.com with kvno 2, encryption type camellia128-cts-cmac added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-servidor.ejemplo.com with kvno 2, encryption type des-hmac-sha1 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-servidor.ejemplo.com with kvno 2, encryption type des-cbc-md5 added to keytab FILE:/etc/krb5.keytab.
```

→ Salimos:

```
kadmin.local:  quit
```

→ Editamos '**/etc/ssh/ssh_config**'

```
GSSAPIAuthentication yes
GSSAPIDelegateCredentials yes
```

→ Editamos '**/etc/ssh/sshd_config**'

```
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
GSSAPIKeyExchange yes
```

→ Reiniciamos 'sshd':

```
# systemctl reload sshd
```

→ Habilitamos el módulo de autenticación kerberos:

```
# yum install pam_krb5
# authconfig --enablekrb5 --update
# which sshd
        /usr/sbin/sshd

# ldd /usr/sbin/sshd |grep -i krb5
libgssapi_krb5.so.2 => /lib64/libgssapi_krb5.so.2 (0x00007fa97b22f000)
libkrb5.so.3 => /lib64/libkrb5.so.3 (0x00007fa97af48000)
libkrb5support.so.0 => /lib64/libkrb5support.so.0 (0x00007fa978c9c000)
```

→ Vemos los puertos definidos:

```
# grep -i kerberos /etc/services
```

→ Instalamos y Habilitamos el firewall:

```
# yum install firewalld
# systemctl start firewalld.service
# systemctl status firewalld.service
# systemctl enable firewalld.service
```

→ → Habilitamos puertos **88/udp** y **88/tcp** para kerberos y **749/tcp** para kadmin :

Creamos plantilla XML '**/etc/firewalld/services/kerberos.xml**' con el contenido:

```
<?xml version="1.0" encoding="utf-8"?>
<service>
<short>Kerberos</short>
<description>Kerberos network authentication protocol
server</description>
<port protocol="tcp" port="88"/>
<port protocol="udp" port="88"/>
<port protocol="tcp" port="749"/>
</service>
```

```
# firewall-cmd --permanent –add-service=kerberos
# firewall-cmd --reload
# firewall-cmd --list-services
dhcpv6-client kerberos ssh
```

→ Probamos configuración para el '**usuario01**':

```
# su – usuario01
$ kinit
Password for usuario01@EJEMPLO.COM:

$ klist
Ticket cache: KEYRING:persistent:1001:1001
```

Default principal: usuario01@EJEMPLO.COM

Valid starting Expires Service principal
04/02/17 09:49:24 05/02/17 09:49:02 krbtgt/EJEMPLO.COM@EJEMPLO.COM

$ ssh kb-servidor.ejemplo.com
Last login: Sat Feb 4 09:52:17 2017 from kb-servidor.ejemplo.com

→ Chequear errores como root:

```
# export KRB5_TRACE=/dev/stdout
# kinit
```

[5871] 1486198547.474705: Getting initial credentials for root@EJEMPLO.COM
[5871] 1486198547.475442: Sending request (183 bytes) to EJEMPLO.COM
[5871] 1486198547.475540: Resolving hostname kb-servidor.ejemplo.com
[5871] 1486198547.478730: Sending initial UDP request to dgram 192.168.100.150:88
[5871] 1486198547.480970: Received answer (169 bytes) from dgram 192.168.100.150:88

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

→ Sincronización del Servidor via NTP (mejor chrony/chronyd daemon).
(Procedemos de forma idéntica como en el Servidor).

→ Cualificación Completa del Servidor (FQDN).

```
# hostnamectl set-hostname kb-cliente.ejemplo.com
# hostnamectl
```
Static hostname: **kb-cliente.ejemplo.com**
Icon name: computer-vm
...

→ Configuraciones: → -**NO-** Configuramos **DNS's** para el ejemplo (red interna):

→ → Contenido '**/etc/hosts**':

...
192.168.100.150 **kb-servidor.ejemplo.com**
192.168.100.151 **kb-cliente.ejemplo.com**
…

→ →Contenido '**/etc/resolv.conf**':

```
# Generated by NetworkManager
search ejemplo.com
nameserver 192.168.100.1
```

→ Paqueteria Necesaria, y habilitación de PAM para kerberos:

```
# yum install -y krb5-workstation pam_krb5
```

→ Copiamos configuración del servidor al cliente:

```
# scp kb-servidor.ejemplo.com:/etc/krb5.conf /etc/krb5.conf
```

→ Creamos 'usuario01':

```
# useradd usuario01
# passwd usuario01
```

→ Añadimos la máquina cliente:

```
[root@kb-cliente carlos]# kadmin usuario01/admin@EJEMPLO.COM
kadmin: Client 'carlos/admin@EJEMPLO.COM' not found in Kerberos database while
initializing kadmin interface
```

→ → **ERROR** → Debemos crear los usuarios adecuados en el Servidor.

→ Ahora en Servidor → '**kb-servidor.ejemplo.com**':

```
[root@kb-servidor carlos]# kadmin.local -q "list_principals"

Authenticating as principal carlos/admin@EJEMPLO.COM with password.
K/M@EJEMPLO.COM
host/kb-servidor.ejemplo.com@EJEMPLO.COM
kadmin/admin@EJEMPLO.COM
kadmin/changepw@EJEMPLO.COM
kadmin/kb-servidor.ejemplo.com@EJEMPLO.COM
kiprop/kb-servidor.ejemplo.com@EJEMPLO.COM
krbtgt/EJEMPLO.COM@EJEMPLO.COM
root/admin@EJEMPLO.COM
usuario01@EJEMPLO.COM

[root@kb-servidor carlos]# kadmin.local -q "addprinc usuario01/admin"

Authenticating as principal carlos/admin@EJEMPLO.COM with password.
WARNING: no policy specified for usuario01/admin@EJEMPLO.COM; defaulting to no
policy
Enter password for principal "usuario01/admin@EJEMPLO.COM":
Re-enter password for principal "usuario01/admin@EJEMPLO.COM":
Principal "usuario01/admin@EJEMPLO.COM" created.
[root@kb-servidor carlos]# kadmin.local -q "list_principals"
Authenticating as principal carlos/admin@EJEMPLO.COM with password.
K/M@EJEMPLO.COM
host/kb-servidor.ejemplo.com@EJEMPLO.COM
```

kadmin/admin@EJEMPLO.COM
kadmin/changepw@EJEMPLO.COM
kadmin/kb-servidor.ejemplo.com@EJEMPLO.COM
kiprop/kb-servidor.ejemplo.com@EJEMPLO.COM
krbtgt/EJEMPLO.COM@EJEMPLO.COM
root/admin@EJEMPLO.COM
usuario01/admin@EJEMPLO.COM
usuario01@EJEMPLO.COM

[root@kb-servidor carlos]# kadmin.local -q "addprinc carlos/admin"

Authenticating as principal carlos/admin@EJEMPLO.COM with password.
WARNING: no policy specified for carlos/admin@EJEMPLO.COM; defaulting to no policy
Enter password for principal "carlos/admin@EJEMPLO.COM":
Re-enter password for principal "carlos/admin@EJEMPLO.COM":
Principal "carlos/admin@EJEMPLO.COM" created.
[root@kb-servidor carlos]# kadmin.local -q "list_principals"
Authenticating as principal carlos/admin@EJEMPLO.COM with password.
K/M@EJEMPLO.COM
carlos/admin@EJEMPLO.COM
host/kb-servidor.ejemplo.com@EJEMPLO.COM
kadmin/admin@EJEMPLO.COM
kadmin/changepw@EJEMPLO.COM
kadmin/kb-servidor.ejemplo.com@EJEMPLO.COM
kiprop/kb-servidor.ejemplo.com@EJEMPLO.COM
krbtgt/EJEMPLO.COM@EJEMPLO.COM
root/admin@EJEMPLO.COM
usuario01/admin@EJEMPLO.COM
usuario01@EJEMPLO.COM

→ Desde Cliente:

[root@kb-cliente carlos]# kadmin

Authenticating as principal carlos/admin@EJEMPLO.COM with password.
Password for carlos/admin@EJEMPLO.COM:

kadmin: addprinc -randkey host/kb-cliente.ejemplo.com

WARNING: no policy specified for host/kb-cliente.ejemplo.com@EJEMPLO.COM; defaulting to no policy
Principal "host/kb-cliente.ejemplo.com@EJEMPLO.COM" created.

kadmin: ktadd host/kb-cliente.ejemplo.com

Entry for principal host/kb-cliente.ejemplo.com with kvno 2, encryption type aes256-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.

Entry for principal host/kb-cliente.ejemplo.com with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-cliente.ejemplo.com with kvno 2, encryption type des3-cbc-sha1 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-cliente.ejemplo.com with kvno 2, encryption type arcfour-hmac added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-cliente.ejemplo.com with kvno 2, encryption type camellia256-cts-cmac added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-cliente.ejemplo.com with kvno 2, encryption type camellia128-cts-cmac added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-cliente.ejemplo.com with kvno 2, encryption type des-hmac-sha1 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kb-cliente.ejemplo.com with kvno 2, encryption type des-cbc-md5 added to keytab FILE:/etc/krb5.keytab.

kadmin: quit

→ Editamos '**/etc/ssh/ssh_config**'

```
GSSAPIAuthentication yes
GSSAPIDelegateCredentials yes
```

→ Editamos '**/etc/ssh/sshd_config**'

```
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
GSSAPIKeyExchange yes
```

→ Reiniciamos Servicios:

```
# systemctl reload sshd
```

→ Habilitamos PAM:

```
# authconfig --enablekrb5 --update
```

→ Testeamos configuración:

```
# su – usuario01

$ kinit
Password for usuario01@EJEMPLO.COM:

[usuario01@kb-cliente ~]$ klist
Ticket cache: KEYRING:persistent:1001:1001
Default principal: usuario01@EJEMPLO.COM
```

Valid starting Expires Service principal
04/02/17 11:18:01 05/02/17 11:17:39 krbtgt/EJEMPLO.COM@EJEMPLO.COM

→ Ya no será necesario repetir la clave:

[usuario01@kb-cliente ~]$ ssh usuario01@kb-servidor.ejemplo.com
Last login: Sun Feb 5 11:30:08 2017 from kb-cliente.ejemplo.com
[usuario01@kb-servidor ~]$

↘ Mostrar slots de 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:

[root@kb-cliente carlos]# **ktutil**
ktutil: **read_kt /etc/krb5.keytab**
ktutil: **l**
slot KVNO Principal
---- ---- ---
1 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM
2 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM
3 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM
4 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM
5 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM
6 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM
7 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM

8 8 host/kb-cliente.ejemplo.com@EJEMPLO.COM
ktutil:

↘ Métodos de Depuración:

[root@kb-cliente carlos]# **/usr/sbin/sshd -d -p 5555**
debug1: sshd version OpenSSH_6.6.1, OpenSSL 1.0.1e-fips 11 Feb 2013
debug1: key_parse_private2: missing begin marker
debug1: read PEM private key done: type RSA
debug1: private host key: #0 type 1 RSA
debug1: key_parse_private2: missing begin marker
debug1: read PEM private key done: type ECDSA
debug1: private host key: #1 type 3 ECDSA
debug1: private host key: #2 type 4 ED25519
debug1: rexec_argv[0]='/usr/sbin/sshd'
debug1: rexec_argv[1]='-d'
debug1: rexec_argv[2]='-p'
debug1: rexec_argv[3]='5555'
Set /proc/self/oom_score_adj from 0 to -1000
debug1: Bind to port 5555 on 0.0.0.0.
Server listening on 0.0.0.0 port 5555.
debug1: Bind to port 5555 on ::.
Server listening on :: port 5555.

[root@kb-cliente carlos]# **ssh -vvv kb-servidor.ejemplo.com -p 5555**

[root@kb-cliente carlos]# **KRB5_TRACE=/dev/stdout kinit aurora**
[3504] 1486895961.130599: Getting initial credentials for aurora@EJEMPLO.COM
[3504] 1486895961.131172: Sending request (185 bytes) to EJEMPLO.COM
[3504] 1486895961.131249: Resolving hostname kb-servidor.ejemplo.com
[3504] 1486895961.132172: Sending initial UDP request to dgram 192.168.100.150:88
[3504] 1486895961.136321: Received answer (254 bytes) from dgram 192.168.100.150:88
[3504] 1486895961.312936: Response was not from master KDC
[3504] 1486895961.313088: Received error from KDC: -1765328359/Additional pre-authentication required
[3504] 1486895961.313264: Processing preauth types: 136, 19, 2, 133
[3504] 1486895961.313308: Selected etype info: etype aes256-cts, salt "EJEMPLO.COMaurora", params ""
[3504] 1486895961.313323: Received cookie: MIT
Password for aurora@EJEMPLO.COM:

3 ==> CONFIGURACIÓN *'DNSMASQ' → kb-servidor.ejemplo.com*

[root@kb-servidor carlos]# yum install dnsmasq

[root@kb-servidor carlos]# systemctl start dnsmasq.service

[root@kb-servidor carlos]# systemctl status dnsmasq.service
[root@kb-servidor carlos]# systemctl enable dnsmasq.service

[root@kb-servidor carlos]# firewall-cmd --add-service=dns --permanent
[root@kb-servidor carlos]# firewall-cmd --reload

→ Contenido '**/etc/hosts**':

192.168.100.150 **kb-servidor.ejemplo.com kb-servidor**
192.168.100.151 **kb-cliente.ejemplo.com kb-cliente**

192.168.100.150 **ejemplo.com**

→ Añadir en '**/etc/dnsmasq.conf**':

no-resolv
server=8.8.8.8
no-poll

→ *Contenido '**/etc/resolv.conf**':*

nameserver 192.168.100.150

→ *Resolución DNS's :*

[root@kb-cliente carlos]# dig kb-servidor.ejemplo.com

; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.1 <<>> kb-servidor.ejemplo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12938
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kb-servidor.ejemplo.com. IN A

;; ANSWER SECTION:
kb-servidor.ejemplo.com. 0 IN A 192.168.100.150

;; Query time: 0 msec
*;; SERVER: **192.168.100.150#53**(**192.168.100.150**)*
;; WHEN: dom feb 12 19:41:46 CET 2017
;; MSG SIZE rcvd: 57

[root@kb-cliente carlos]# dig kb-cliente.ejemplo.com

; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.1 <<>> kb-cliente.ejemplo.com

;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40971
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kb-cliente.ejemplo.com. IN A

;; ANSWER SECTION:
kb-cliente.ejemplo.com. 0 IN A 192.168.100.151

;; Query time: 1 msec
*;; SERVER: **192.168.100.150#53**(**192.168.100.150**)*
;; WHEN: dom feb 12 19:54:52 CET 2017
;; MSG SIZE rcvd: 56

4 ==> CONFIGURACIÓN '*DNSMASQ*' → *kb-cliente.ejemplo.com*

→ *Contenido '**/etc/hosts**' :*

*192.168.100.150 **kb-servidor.ejemplo.com kb-servidor***
*192.168.100.151 **kb-cliente.ejemplo.com kb-cliente***

→ *Contenido '**/etc/resolv.conf**' :*

nameserver 192.168.100.150

→ *Resolución DNS's :*

[root@kb-cliente carlos]# dig kb-servidor.ejemplo.com

; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.1 <<>> kb-servidor.ejemplo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12938
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kb-servidor.ejemplo.com. IN A

;; ANSWER SECTION:
kb-servidor.ejemplo.com. 0 IN A 192.168.100.150

;; Query time: 0 msec

*;; SERVER: **192.168.100.150#53**(**192.168.100.150**)*
;; WHEN: dom feb 12 19:41:46 CET 2017
;; MSG SIZE rcvd: 57

[root@kb-cliente carlos]# dig kb-cliente.ejemplo.com

; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.1 <<>> kb-cliente.ejemplo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40971
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kb-cliente.ejemplo.com. IN A

;; ANSWER SECTION:
kb-cliente.ejemplo.com. 0 IN A 192.168.100.151

;; Query time: 1 msec
*;; SERVER: **192.168.100.150#53**(**192.168.100.150**)*
;; WHEN: dom feb 12 19:54:52 CET 2017
;; MSG SIZE rcvd: 56

BIBLIOGRAFIA:

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