ANEXO 3: NTP

Índice general

Capítulo 1

NTP

Contents

En una red donde se replican bases de datos (o, también, donde se expiden tickets que proveen memoria al estado de autenticación de una entidad pero que presentan fecha de caducidad) es crítico que los relojes de las máquinas permanezcan sincronizados[1]. Idealmente, esa sincronización se dará además con una fuente de hora reconocida internacionalmente. El protocolo que lo permite es NTP[2] descrito en el rfc5905.

Desplegaremos dos servidores de tiempo (uno en dklab1, otro en dklab2) configurados en modo "Simétrico activo/pasivo (unicast peers)" en asociación permanente pero con posibilidad de pseudodescubrimiento de servicio "Orphan Mode", y los servicios de seguridad los proveerá el subprotocolo Autokey v2 esquema IFF (basado en criptografía asimétrica). Además pueden sincronizarse (ser clientes de un stratum inferior) con servidores que usen (o no) Autokey igualmente.

De otro lado, sus clientes verán, en asociación permanente, a servidores unicast con descubrimiento de servicio tipo pool.

La implementación de NTP que permite todas estas características es la de NTP Proyect ntp.org.[3]

1.1. DKLAB1

1.1.1. Instalación y configuración

```
apt-get install ntp
# hace algunos an~os se instalaba a ntpdate como cliente, pero su
# comportamiento es reproducible con el propio ntpd
# (en concreto, ntpd -q -g)

man ntp.conf
```

Vamos a configurarlo editando /etc/ntpd.conf:

```
vim /etc/ntp.conf
```

- Anotación: ntp.conf permite la inclusión de ficheros con "includefile <pathfile>", mecanismo que por claridad de exposición no usamos pero que conviene utilizar.

[1] No en sentido literal, pero del orden de ms. (Hoy sabemos, además, que no existe en el mundo físico ese sentido literal: según la Teoría de la Relatividad no existe la simultaneidad de sucesos).

[2] http://support.ntp.org/bin/view/Main/WebHome#What_is_NTP_Network_Time_Protoco

[3] Dicho proyecto permite, además de lo expuesto, la posibilidad de utilizar un dispositivo GPS como fuente de tiempo stratum 0. Se requiere hardware adicional y por tanto no se abordará esta opción.

```
driftfile /var/lib/ntp/ntp.drift

####fx:
enable stats
statsdir "/var/log/ntpstats"
#-statistics loopstats peerstats clockstats
statistics cryptostats
filegen cryptostats file cryptostats type none enable
####endfx
filegen loopstats file loopstats type day enable
...

####fx:
keysdir /etc/ntp/crypto
crypto randfile /dev/urandom   # u'til si en syslog:
                               #  crypto_setup: random seed file not found
crypto host dklab1.casafx.dyndns.org # identificador del host
crypto ident casafx.dyndns.org # nombre del grupo IFF, si pertenecemos a uno.
crypto pw ntpautokey           # passphrase de las llaves privadas
                               # Nota: host e ident hace que se busquen
                               # unos ficheros u otros en keysdir, nada ma's.

# Modo sime'trico activo/pasivo (unicast peers)
peer dklab2.casafx.dyndns.org autokey
restrict dklab2.casafx.dyndns.org notrust

# Pseudodescubrimiento de servicio Orphan mode, si no alcanzable stratum >5
tos orphan 5
```

```
# Servidores de menor stratum con los que sincronizarse:
#  Cua'les, si con Autokey, de que' stratum:
#  Existe un buscador en ntp.org:
#  http://support.ntp.org/bin/view/Servers/WebHome
#  (con varios criterios de bu'squeda: stratum, poli'tica de uso...).
#  http://support.ntp.org/bin/view/Servers/ServersAuthenticatedWithAutokey
#  (con autokey).
#  Nota sobre stratum:
#       ntpq -p en el campo "st" nos dice a que' stratum pertenece cada fuente,
#       lo anuncia inteligentemente el driver correspondiente del ntpd remoto.
#       Existe una opcio'n para redeclararlo a mano, siendo un valor seguro 10:
#        server <name> ...
#        fudge <name> stratum 10
#       Tu stratum depende de la fuente seleccionada en cada momento, se
#       consulta con el comando ntptrace, en concreto sera' el que diga para
#       el extremo inicial de la traza ( localhost ).
#
```

```
#  Ejem de sincronizacio'n a servidor remoto con autokey:
#  0) NO funcionara' tras NAT (por ello no lo pudimos comprobar y se deja esta nota
#  1) Encue'ntrese un servidor que utilice autokey y sea de acceso pu'blico:
#     Ejem: http://support.ntp.org/bin/view/Servers/RacketyUdelEdu (stratum 1)
#  2) Decla'rese aqui' en el ntp.conf:
#     server rackety.udel.edu iburst autokey
#     restrict rackety.udel.edu notrust nomodify notrap ntpport
#  Nota) no es el caso porque ya pertenecemos a un grupo (casafx.dyndns.org)
#        pero si quisie'ramos formar parte de su grupo en lugar del nuestro,
#        podri'amos adicionalmente:
#        -Desca'rguese sus IFF parameters (clave DSA):
#         En el ejem viene incrustada en la web, otras veces hay un enlace...
#          w3m -dump http://support.ntp.org/bin/view/Servers/RacketyUdelEdu \
#              | tail -n +8| head -9 \
#              >/etc/ntp/crypto/ntpkey_iffpar_rackety.3401120457
#          ln -s /etc/ntp/crypto/ntpkey_iffpar_rackety.3401120457 \
#                /etc/ntp/crypto/ntpkey_iffpar_rackety
#        -Anu'nciese el cambio de grupo en el ntp.conf: crypto ident rackety
```

```
#...otros servidores (sin autokey) bien podri'an ser los provei'dos por debian:
#   (por ejemplo al pool "3.debian.pool.ntp.org" pertenece el stratum 1
#   hora.cica.es en Sevilla):
####endfx
...
server 0.debian.pool.ntp.org iburst
server 1.debian.pool.ntp.org iburst
server 2.debian.pool.ntp.org iburst
server 3.debian.pool.ntp.org iburst
...
```

Autorización:

Para que otros equipos de la red tengan a dklab1/2 como servidores de hora, no hace falta modificar nada puesto que la política por defecto permite que ntpd responda a quien quiera que le pregunte por la hora. Así, si volvemos a echar un vistazo al ntp.conf podremos ver la sección con las ACL[4] sobre autorización:

```
view /etc/ntp.conf
```

```
...
# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery
# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1
...
```

Aclaramos que noquery no afecta a servir la hora, sólo a que se conecten ntpq o ntpdc desde otra interfaz que no sea la de retorno, la IP de origen127.0.0.1 o su versión para

[4] http://support.ntp.org/bin/view/Support/AccessRestrictions

IPv6.

Rotación del log para cryptostats

Para comprobar el funcionamiento de autokey tuvimos que activar el sistema de logs en el ntp.conf; cuando todo funcione correctamente, podemos desactivarlo o configurar al rotador de logs del sistema:

```
vim /etc/logrotate.d/ntp
```

```
####fx:
/var/log/nptstats/cryptostats {
 daily
 missingok
 rotate 7
 compress
 delaycompress
 #notifempty
}
####endfx
```

1.1.2. Generación del material criptográfico para autokey v2 IFF

Vamos con el material criptográfico. Debemos generar los parámetros del esquema IFF (una llave DSA) junto a un par llave pública y llave privada (un par RSA). Utilizamos ntp-keygen:

```
mkdir -p /etc/ntp/crypto

chown ntp:root /etc/ntp/crypto

cd /etc/ntp/crypto

I="-i casafx.dyndns.org"

H="-s dklab1.casafx.dyndns.org"

ntp-keygen $H $I -T -I -p ntpautokey


ls
```

- -T para hacer incluir la extensión "X509v3 Extended Key Usage" con el valor "Trust Root", el cual permite que el certificado sea interpretado como del "NTP Trust Group", la TA (Time Authority). Por defecto el grupo para el que se crea el material criptográfico tiene como identificador al nombre dado al host (lo que devuelva gethostname() o, mejor, lo que declaremos con -s <estehost>), ésto nos obliga a añadir -i <estehost>en el resto de peers o, para no llevar a confusión, hacer en todos los peers -i <groupname>.
- -i para el nombre del grupo. El argumento de -i para ntp-keygen debe coincidir con el de "crypto ident" en ntp.conf. Además será el valor del Common Name (Issuer y Subject) en los certificados x509 (sólo en certificados autofirmados para clientes es el hostname el valor del Common Name).
    - Nota: los nombres de host y group no son objeto de verificación DNS etc, son valores independientes para la autentificación en autokey[5].
- -s para el nombre de host. El argumento de -s para ntp-keygen debe ser el de "crypto host" en ntp.conf.
- -I para crear la llave IFF.

Genera un par RSA, y una llave DSA. Aún debemos exportar la group key con los parámetros IFF que compartir (sin passpharase) así:

```
ntp-keygen $H $I -e -q ntpautokey -p ntpautokey > ntp_trust_group_key
```

Es público, se maneja como una llave pública (la podemos distribuir en la web etc). La diferencia (con la llave DSA ntpkey_IFFkey) es que no tiene passphrase. Y no se pide si lo usamos:

[5] Consúltese file://usr/share/doc/ntp-doc/html/keygen.html

```
openssl dsa -text -in ntp_trust_group_key
```

La llave de grupo hay que transferirla y enlazarla a todos los ntpd que vayan a usar autokey: dklab1 y dklab2.

```
groupkey=‘head -n 1 ntp_trust_group_key | sed s/#\ //g‘
cp ntp_trust_group_key $groupkey
ln -s $groupkey ntpkey_iffpar_casafx.dyndns.org
```

Debiéramos hacer legible el material criptográfico a ntp y no a otros:

```
chown -R ntp:root /etc/ntp/crypto
chmod -R o-rwx /etc/ntp/crypto

chown ntp:root /etc/ntp.conf
chmod o-rwx /etc/ntp.conf
```

Renovación

Los parámetros caducan al año por defecto. Su renovación obliga a actualizar el certificado también.

```
ntp-keygen -s dklab1.casafx.dyndns.org -i casafx.dyndns.org \
           -T -q ‘awk ’/crypto pw/ { print $3 }’ </etc/ntp.conf‘
```

Es conveniente conocer que algunos flags de ntp-keygen podemos tenerlos disponibles en variables (NTP_KEYGEN_*) o, mejor, almacenados en rc-files: /root/.ntprc o /etc/ntp/crypto/.ntprc. Podemos hacer que ntp-keygen nos muestre el formato de esos ficheros con la opción ’>’:

```
ntp-keygen -T -I -s host -i group -c RSA-MD5 -m 1024 \
           -p pass ’->’ rc-example; cat rc-example
```

1.1.3. Reinicio del servicio

```
invoke-rc.d ntp restart
```

Más tarde, cuando hayamos desplegado en dklab2, realizaremos las comprobaciones reelevantes.

1.2. DKLAB2

1.2.1. Instalación y configuración

```
apt-get install ntp
```

- Anotación: ahora que estamos desplegando el segundo servidor, podemos comentar que idealemten (y en el año 2003[6]) se decía que "the rule of thumb" correspondía a 1 servidor ntp por cada 12 clientes, pero ésto dependerá de cada caso y cualidad de los medios disponibles.

Vamos con la configuración.

- Anotación: nuestro esquema (peers utilizando autokey v2) es compatible según la tabla http://www.linuxcertif.com/man/5/ntp_auth/#IDENTITY_SCHEMES_AND_CRYPTOTYPES_

```
vim /etc/ntp.conf
```

[6] http://osr507doc.sco.com/en/NetAdminG/ntpC.guidelines.html

```
driftfile /var/lib/ntp/ntp.drift

####fx:
enable stats
statsdir "/var/log/ntpstats"
#-statistics loopstats peerstats clockstats
statistics cryptostats
filegen cryptostats file cryptostats type none enable
####endfx
filegen loopstats file loopstats type day enable
...

####fx:
keysdir /etc/ntp/crypto
crypto randfile /dev/urandom   # u'til si en syslog:
                               #  crypto_setup: random seed file not found
crypto host dklab2.casafx.dyndns.org # identificador del host
crypto ident casafx.dyndns.org # nombre del grupo IFF
crypto pw ntpautokey           # passphrase de las llaves privadas

# Modo sime'trico activo/pasivo (unicast peers)
peer dklab1.casafx.dyndns.org autokey
restrict dklab1.casafx.dyndns.org notrust

# Pseudodescubrimiento de servicio Orphan mode, si no alcanzable stratum >5
tos orphan 5
```

```
# Servidores de menor stratum con los que sincronizarse:
#  Cua'les, si con Autokey, de que' stratum:
#  Existe un buscador en ntp.org,
#  http://support.ntp.org/bin/view/Servers/WebHome
#  (stratum, poli'tica de uso...)
#  http://support.ntp.org/bin/view/Servers/ServersAuthenticatedWithAutokey
#  (con autokey)
#  Nota sobre stratum:
#       ntpq -p en el campo "st" nos dice a que' stratum pertenece cada fuente,
#       lo anuncia inteligentemente el driver correspondiente del ntpd remoto.
#       Existe una opcio'n para redeclararlo a mano, siendo un valor seguro 10:
#        server <name> ...
#        fudge <name> stratum 10
#       Nuestro stratum depende de la fuente seleccionada en cada momento, se
#       consulta con ntptrace, en concreto sera' el que diga para el
#       extremo inicial de la traza ( localhost ).
#
```

```
#  Ejemplo de sincronizacio'n a servidor remoto con autokey:
#  0) NO funcionara' si tras NAT (por ello no se pudo comprobar).
#  1) Encue'ntrese servidor que utilice autokey y sea de acceso pu'blico:
#     Ejemplo: http://support.ntp.org/bin/view/Servers/RacketyUdelEdu
#     (stratum 1)
#  2) Decla'rese aqui' en el ntp.conf:
#     server rackety.udel.edu iburst autokey
#     restrict rackety.udel.edu notrust nomodify notrap ntpport
#  Nota) no es el caso porque ya pertenecemos a un grupo
#        (casafx.dyndns.org)
#        pero si quisie'ramos formar parte de su grupo en lugar del nuestro,
#        podri'amos adema's:
#        -Descargar sus IFF parameters (clave DSA):
#         En el ejem viene incrustada en la web, otras veces hay un enlace...
#         w3m -dump http://support.ntp.org/bin/view/Servers/RacketyUdelEdu\
#             | tail -n +8| head -9 \
#             >/etc/ntp/crypto/ntpkey_iffpar_rackety.3401120457
#         ln -s /etc/ntp/crypto/ntpkey_iffpar_rackety.3401120457 \
#         /etc/ntp/crypto/ntpkey_iffpar_rackety
#        -Anu'nciese el cambio de grupo en el ntp.conf: crypto ident rackety
```

```
#...otros servidores (sin autokey) bien podri'an ser los provei'dos por debian:
#   (por ejemplo al pool "3.debian.pool.ntp.org" pertenece el stratum 1
#   hora.cica.es en Sevilla):
####endfx
...
server 0.debian.pool.ntp.org iburst
server 1.debian.pool.ntp.org iburst
server 2.debian.pool.ntp.org iburst
server 3.debian.pool.ntp.org iburst
...
```

Autorización:

Como se indicó al desplegar en dklab1, para que otros equipos de la red tengan a dklab1/2 como servidores de hora, no hace falta modificar nada puesto que la política por defecto permite que ntpd responda a quien quiera que le pregunte por la hora. Así, si volvíamos a echar un vistazo al ntp.conf podíamos ver la sección con las ACL[7] sobre autorización:

```
view /etc/ntp.conf
```

```
...
# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery
# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1
...
```

Y como se comentó, "noquery" no afecta a servir la hora, sólo a que se conecten ntpq o ntpdc (no lo permite más que localmente).

[7] http://support.ntp.org/bin/view/Support/AccessRestrictions

Rotación del log para cryptostats

```
vim /etc/logrotate.d/ntp
```

```
####fx:
/var/log/nptstats/cryptostats {
 daily
 missingok
 rotate 7
 compress
 delaycompress
 #notifempty
}
####endfx
```

1.2.2. Obtención del material criptográfico

```
mkdir -p /etc/ntp/crypto
chown ntp:root /etc/ntp/crypto
cd /etc/ntp/crypto
```

Hago que ambos hosts tengan el mismo material criptográfico de TA (Time Authority):

- Anotación: al ser TA, los certificados tienen como Subject e Issuer el grupo, y puesto que es común, no genera incompatibilidad. Sí hay, por supuesto, que renombrar los archivos acorde a lo declarado en el ntp.conf. Esta solución es la única que ha funcionado y, puesto que no hay howto's para el esquema Peers+IFF, sospecho que quizás sea lo correcto. La lectura del paper "The Autokey Security Architecture, Protocol and Algorithms" en http://www.eecis.udel.edu/~mills/database/reports/stime1/stime.pdf no modificó la situación, aunque es la fuente definitiva para entender el diseño del subprotocolo autokey v2 de NTP.

```
ssh 10.168.1.1 "(cd /etc/ntp/crypto; tar -cvf - ./)" | cat > k.tar
tar -xf k.tar
rm k.tar
for i in ntpkey_cert* ntpkey_host* ntpkey_RSAhost* ntpkey_RSA-MD5cert*
 do dklab1=‘ls $i‘
    dklab2=‘echo $dklab1 | sed s/dklab1/dklab2/g‘
    echo echo $dklab1 $dklab2
    mv $dklab1 $dklab2
    if echo $dklab1 | grep MD5cert
     then ln --force -s $dklab2 ntpkey_cert_dklab2.casafx.dyndns.org
    elif echo $dklab1 | grep RSAhost
     then ln --force -s $dklab2 ntpkey_host_dklab2.casafx.dyndns.org
    fi
done
```

Vuelven a ser válidas las recomendaciones que se dieron sobre la renovación al año. Respecto a los permisos:

```
chown -R ntp:root /etc/ntp/crypto
chmod -R o-rwx /etc/ntp/crypto

chown ntp:root /etc/ntp.conf
chmod o-rwx /etc/ntp.conf
```

1.2.3. Reinicio del servicio

```
invoke-rc.d ntp restart
```

1.3. Tests

Utilizamos el software ntpd (sí, también tiene la funcionalidad de cliente), ntpq (para inspeccionar sobre el estado de sincronización con los demás servidores NTP) y ntptrace (sigue una cadena de sincronización de servidores NTP hasta su stratum 0). También existe ntpdc que inspecciona a ntpd en sí y no nos es interesante ahora. La salida de los programas se organiza en distintas columnas, y se hace necesaria una leyenda para interpretarlas:

- ntpq -pn

```
()remote           refid      st t when poll reach   delay   offset  jitter
: :                :          :  : :    :    :       :       :       ‘->/\ms entre 2 samples
: :                :          :  : :    :    :       :       ‘->/\ms entre cl/srv
: :                :          :  : :    :    :       ‘->tiempo de ronda para recibir respuesta
: :                :          :  : :    :    ‘->si alcanzable 377=siempre
: :                :          :  : :    ‘->poll interval
: :                :          :  : ‘->segundos desde u’ltima respuesta
: :                :          :  ‘->tipo:
: :                :          ‘->stratum
: :                ‘->fuente actual pero del remoto
: ‘->host fuente
‘->seleccio’n: *actual, +seleccionado al menos, -descartado al elegir, ()descartado quiza’s err
```

- ntpq -c as

```
ind assid status  conf reach auth condition  last_event cnt
:   :     :       :    :     :    :          :          ‘->
:   :     :       :    :     :    :          ‘->
:   :     :       :    :     :    ‘->si se usa ese server o no (reject)
:   :     :       :    :     ‘->ok es que se usa y none que no, sin ma’s creo
:   :     :       :    ‘->
:   :     :       ‘->
:   :     ‘->status word del peer, que se decodifica a las siguientes
:   ‘->association identificator
‘->i’ndice uso interno
```

- ntptrace es autoexplicativo.

Según las ACL, podemos sincronizar el reloj desde cualquier host:

```
ntpd -q -g
```

Sólo desde localhost podemos conectarnos e inspeccionar el servidor en sí con ntpdc:

```
ntpdc -c sysinfo localhost # ntpdc localhost para que
                           # de' prompt interactivo
```

Podemos comprobar que se asocia con los servers/peers indicados e intercambia paquetes (el que lleve el '*én la columna 0 es nuestra fuente de hora seleccionada actual):

```
ntpq -p localhost
ntpq -c "rv 0 cert"
ntpdc -nc pe localhost
```

Podemos seguir hacia atrás la cadena de fuentes de hora hasta el stratum 0, y adicionalmente nos da cuál es nuestro stratum actual (el de 127.0.0.1).

```
ntptrace -n # -n para que no intente hacer resoluciones DNS inversas
```

Para ver el estado de las autenticaciones que efectúa, y puesto que activamos la opción cryptolog, podemos inspeccionar el fichero:

```
cat /var/log/ntpstats/cryptostats
```

```
55767 50947.877 0.0.0.0 ntpkey_RSAhost_dklabX.casafx.dyndns.org.3520590599 mod 512
55767 50947.877 0.0.0.0
      ntpkey_RSA-MD5cert_dklabX.casafx.dyndns.org.3520590599 0x1 len 356
55767 50947.877 0.0.0.0 ntpkey_IFFkey_casafx.dyndns.org.3520590599 mod 384
55767 50947.877 0.0.0.0 setup 0x80021 host dklabX.casafx.dyndns.org
      md5WithRSAEncryption
55767 50948.881 0.0.0.0 signature update ts 3520591748
55767 50949.673 10.168.1.2 assoc 16480 11723 host casafx.dyndns.org
      md5WithRSAEncryption
55767 50952.677 0.0.0.0 signature update ts 3520591752
55767 50952.677 10.168.1.2 cert casafx.dyndns.org casafx.dyndns.org 0x5
      md5WithRSAEncryption (8) fs 3520590599
55767 50953.873 10.168.1.2 ntpkey_iffpar_casafx.dyndns.org.3520590599 mod 384
55767 50955.679 10.168.1.2 iff casafx.dyndns.org fs 3520590599
55767 50958.675 10.168.1.2 cook 85e807bb ts 3520591758 fs 3520591753
```

... la última línea indica que se creó la cookie, cuando ésto sucede el host remoto pasa al estado "reacheable", véase a continuación "ntpq -cas". El log anterior sigue con:

```
55767 50961.673 10.168.1.2 auto seq 64 key 9c1fb526 ts 3520591761 fs 3520591753
55767 50964.681 0.0.0.0 signature update ts 3520591764
55767 50964.681 10.168.1.2 sign casafx.dyndns.org casafx.dyndns.org 0x5
      md5WithRSAEncryption (8) fs 3520590599
```

... la última línea indica que se ha firmado al vuelo, como caracteriza al esquema de autenticación usado.

Podemos usar ntpq -c as para comprobar si está utilizando autenticación. Auth "ok" es que la usa. Condition "reject" es que no lo usa porque hay algún problema.

```
ntpq -c as localhost
ntpq -c "rv <assID>"
ntpq -c "rv <assID> flags"
```

Usando la columna assID podemos profundizar algo más:

```
ntpq -c "rv <assID>"
ntpq -c "rv <assID> flags"
```

...flags=0x84021, su interpretación está en el código fuente, puede también consultarse o aquí (al final).

Si, mediante cualquier medio, aislamos ambos ntpd de sus servidores remotos, se activa el modo orphan, dando "ntpq -p" un stratum de >=5 (en relación a "toc orphan 5" en ntp.conf. Uno de ellos tendrá una * para el otro, lo que indica quién se está sincronizando de quién en ese momento. Sería algo como (en este ejemplo dklab1 toma el mando):

```
ntpq -p
```

```
*dklab1.casafx.dyndns.org 127.0.0.1        5 ...
```

```
ntpq -p
```

```
dklab2.casafx.dyndns.org 10.168.1.1       6 ...
```

Pueden repetirse los tests para dklab2. LyX