http://www.cnblogs.com/morvenhuang/p/4607790.html

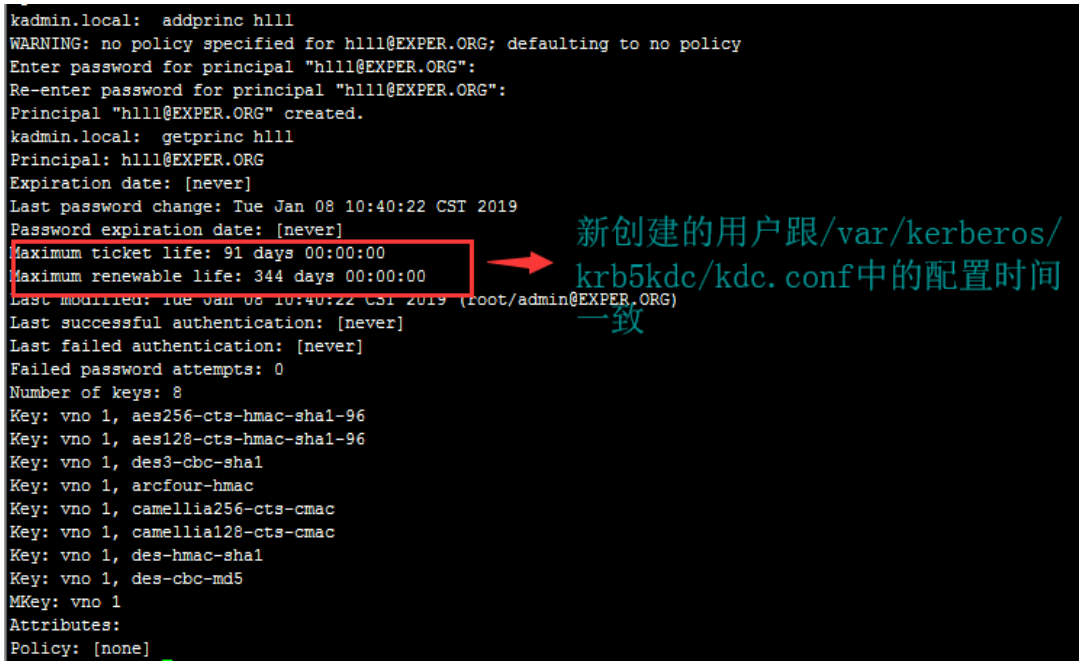
https://linux.die.net/man/5/krb5.conf

有效期和续订期设置

https://blog.csdn.net/yinansheng1/article/details/79397309

systemctl restart kadmin

systemctl restart krb5kdc



/etc/krb5.conf

[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
 # renewable = true
 rdns = false
 default_realm = DEVDIP.ORG
 default_ccache_name = KEYRING:persistent:%{uid}
 dns_fallback = no
 dns_lookup_kdc = true
 udp_preference_limit = 1
[realms]
 DEVDIP.ORG = {
    admin_server = dev-dmp1.fengdai.org
    kdc = dev-dmp1.fengdai.org
 }
 TESTDIP.ORG = {
  kdc = test-dmp1.fengdai.org
  admin_server = test-dmp1.fengdai.org
  max_renewable_life = 7d 0h 0m 0s
  default_principal_flags = +renewable
 }
 PRODDIP.ORG = {
   kdc = tcp/prod-dmp11.fengdai.org:88
   admin_server = prod-dmp11.fengdai.org
 }
[domain_realm]
 .exper.org = DEVDIP.ORG
  exper.org = DEVDIP.ORG
  testdip.com = TESTDIP.ORG
  proddip.org = PRODDIP.ORG
```

/var/kerberos/krb5kdc/kdc.conf

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

[realms]
  DEVDIP.ORG = {
  max_life = 24h
  max_renewable_life = 7d
  default_principal_flags = +renewable
  #master_key_type = aes256-cts
  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
 }
```

ticket_lifetime = 24h

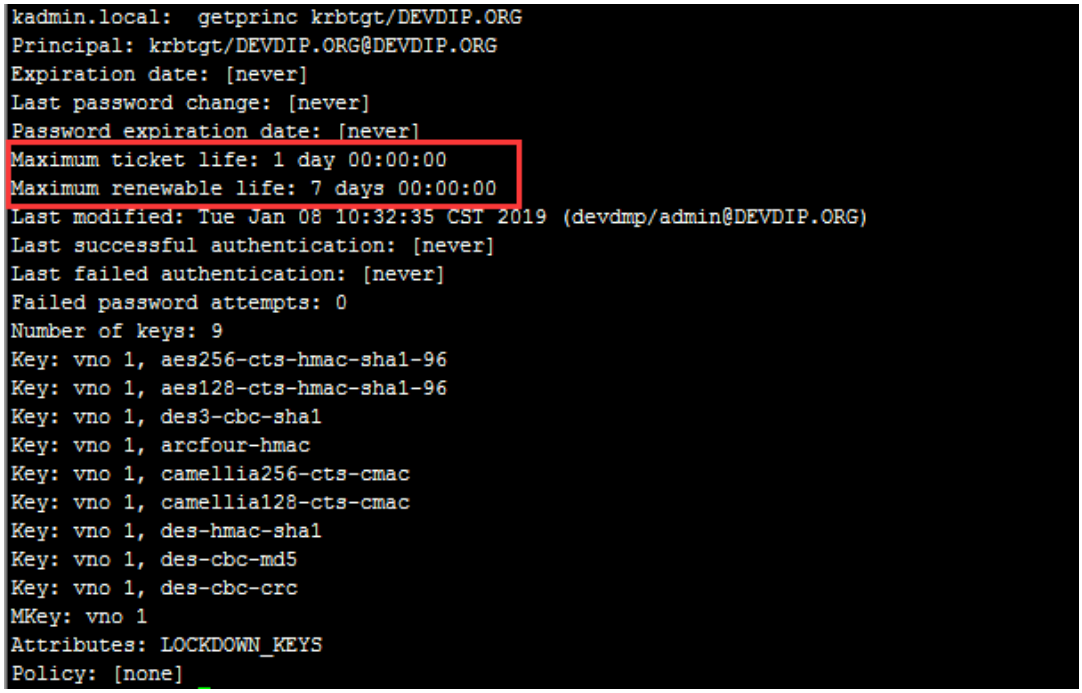
ticket 具有lifetime（生命周期），超过设置的时间ticket就会过期，需要重新申请renew。

ticket lifetime 取决于以下配置项中的最小值

1. kerberos server上的/var/kerberos/krb5kdc/kdc.conf中的max-file

```
  max_life = 24h
```

2.内置principal krbtgt的maximum ticket life，可在kadmin命令行下用getprinc命令查看



modprinc -maxlife 24h krbtgt/DEVDIP.ORG

modprinc -maxrenewlife 7d krbtgt/DEVDIP.ORG

getprinc krbtgt/DEVDIP.ORG

3.你的principal的maximum ticket life，可在kadmin命令行下用getprinc命令查看

kadmin.local: getprinc fengkong

Principal: fengkong@DEVDIP.ORG

Expiration date: [never]

Last password change: Mon Dec 03 09:47:11 CST 2018

Password expiration date: [never]

Maximum ticket life: 1 day 00:00:00

Maximum renewable life: 7 days 00:00:00

Last modified: Mon Dec 03 09:47:11 CST 2018 (root/admin@DEVDIP.ORG)

Last successful authentication: [never]

Last failed authentication: [never]

Failed password attempts: 0

Number of keys: 8

Key: vno 1, aes256-cts-hmac-sha1-96

Key: vno 1, aes128-cts-hmac-sha1-96
Key: vno 1, des3-cbc-sha1
Key: vno 1, arcfour-hmac
Key: vno 1, camellia256-cts-cmac
Key: vno 1, camellia128-cts-cmac
Key: vno 1, des-hmac-sha1
Key: vno 1, des-cbc-md5
MKey: vno 1
Attributes:
Policy: [none]

4.Kerberos client上/etc/krb5.conf的 ticket_lifetime

ticket_lifetime = 24h

5.kinit -l 参数后面指定的时间

-l lifetime

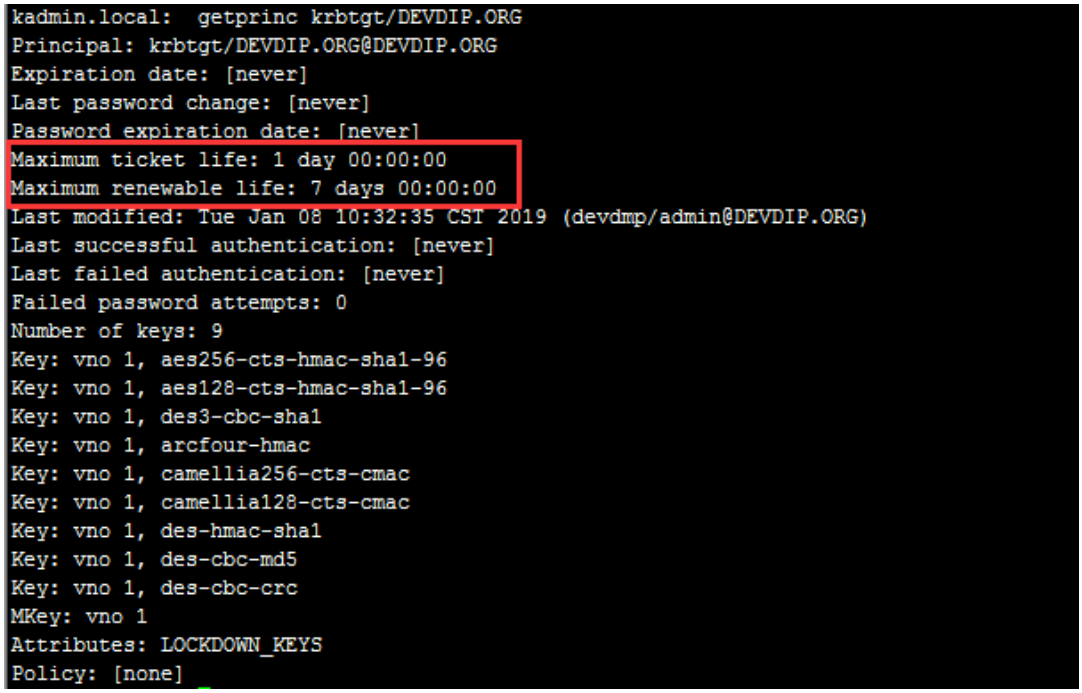
renew_lifetime = 7d

ticket过期后，如果想延长，一种方法是重新申请（需要输入密码），另一种是renew（不需要输入密码），每renew一次，就延长一个lifetime。不过renew操作本身也有lifetime，即在ticket renew lifetime，在此lifetime之内，才能进行renew操作。与上面的很相似，ticket renew lifetime取决于以下5项设置中的最小值：

1. kerberos server上的/var/kerberos/krb5kdc/kdc.conf中的max_renewable_life

max_renewable_life = 7d

2.内置principal krbtgt的maximum renewable life，可在kadmin命令行下用getprinc命令查看



3.你的principal的maximum renewable life，可在kadmin命令行下用getprinc命令查看

kadmin.local: getprinc fengkong

Principal: fengkong@DEVDIP.ORG

Expiration date: [never]

Last password change: Mon Dec 03 09:47:11 CST 2018

Password expiration date: [never]

Maximum ticket life: 1 day 00:00:00

Maximum renewable life: 7 days 00:00:00

Last modified: Mon Dec 03 09:47:11 CST 2018 (root/admin@DEVDIP.ORG)

Last successful authentication: [never]

Last failed authentication: [never]

Failed password attempts: 0

Number of keys: 8

Key: vno 1, aes256-cts-hmac-sha1-96

Key: vno 1, aes128-cts-hmac-sha1-96

Key: vno 1, des3-cbc-sha1

Key: vno 1, arcfour-hmac

Key: vno 1, camellia256-cts-cmac

Key: vno 1, camellia128-cts-cmac

Key: vno 1, des-hmac-sha1

Key: vno 1, des-cbc-md5

MKey: vno 1

Attributes:

Policy: [none]

4.Kerberos client上/etc/krb5.conf的renew_lifetime

renew_lifetime = 7d

5.kinit -r 参数后面指定的时间

-r renewable lifetime

udp_preference_limit = 1

表示始终使用TCP协议

当向KDC发送消息时，如果消息的大小高于udp_preference_limit，则库将尝试在UDP之前使用TCP 。如果消息小于 udp_preference_limit，则将在TCP之前尝试UDP。无论大小如何，如果第一次尝试失败，将尝试两种协议

ticket_lifetime

表明凭证生效的时限，一般为24小时。初始票证的默认生存期

renew_lifetime

表明凭证最长可以被延期的时限，一般为一个礼拜。当凭证过期之后，对安全认证的服务的后续访问则会失败。初始票证的默认可更新生命周期

forwardable = true

设置所有tickets中的可转发标志，允许用户将其凭据从一个主机转移到另一个主机而无需重新进行身份验证，也可以在APPdefaults或realms中设置，以限制其在特定应用程序中的使用或仅限于特定领域

renewable = true

可以续订的TGT（在tickets到期之前）

rdns = false

false 表示将主机名转换为服务主体名称时阻止使用反向DNS解析，默认为true，false更安全，但可能会强制用户在对服务进行身份验证时专门使用完全限定的域名

default_ccache_name = KEYRING:persistent:%{uid}

默认凭证缓存的名称

dns_fallback = no

控制DNS用于kerberos信息的通用标志，如果指定了dns_lookup_kdc，dns_lookup_realm，则该配置无效

dns_lookup_kdc = true

拒绝服务攻击，定位域的kdc，请注意，admin_server条目必须位于krb5.conf领域信息中才能联系kadmind，因为kadmin的DNS实现不完整

指示是否需要使用DNS SRV记录来定位KDC和域的其他服务器（如果它们尚未在[realms]部分中列出）。如果somone欺骗DNS记录并重定向到另一台服务器，则此选项会使计算机容易受到某种类型的DoS攻击。然而，这并不比DoS差，因为伪造的KDC无法解码所发送的任何内容（初始票证请求除外，它没有加密数据）。此外，假冒KDC发出的任何内容都不会在没有验证的情况下被信任（本地机器不知道要使用的密钥）。如果未指定dns_lookup_kdc但dns_fallback为，则使用该值。在任何一种情况下，[领域]中的值（如果存在）部分覆盖DNS。默认情况下启用dns_lookup_kdc

dns_lookup_realm = false

查找回退主机到域的映射和默认域的DNS记录，为true时，运行

指示是否需要使用DNS TXT记录来确定主机的Kerberos域信息和/或主机/域名到域的映射（如果该信息尚未存在于krb5.conf文件中）。启用此选项可能会使主机容易受到重定向攻击，其中欺骗性DNS回复说服客户端对错误的域进行身份验证。在没有跨领域信任的领域，这是一个DoS攻击。如果未指定dns_lookup_realm但dns_fallback为，则使用该值。在任何一种情况下，[libdefaults]和[domain_realm]

部分中的值（如果存在）都会覆盖DNS

default_realm

标识客户端的默认kerberos域，如果没有设置该项，则在kinit时需要指定主体的域

default_tgs_enctypes

此关系标识应由KDC返回的受支持的会话密钥加密类型列表。列表可以用逗号或空格分隔。

default_tkt_enctypes

此关系以相同的格式标识客户端应该请求的受支持的会话密钥加密类型列表

noaddresses

设置此标志会导致初始kerberos票证无地址，默认为true

false 可转发 代理

encryption 加密类型：

- des-cbc-md5
- des-cbc-crc
- des3-cbc-sha1
- rc4-hmac
- arcfour-hmac
- arcfour-hmac-md5
- aes128-cts-hmac-sha1-96
- aes256-cts-hmac-sha1-96

tickets

```
[root@dev-dmp7 bin]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: dmpadmin@DEVDIP.ORG

Valid starting       Expires              Service principal
01/07/2019 15:01:27  01/08/2019 15:01:27  krbtgt/DEVDIP.ORG@DEVDIP.ORG
        renew until 01/14/2019 15:01:27
```

valid starting：有效起始

expires:过期

这两个设置描述了tickets的有效的时间段，主要描述了每张票，票证授予票证具有主票证 krbtgt，实例是域名

```
[root@dev-dmp7 bin]# klist -f
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: dmpadmin@DEVDIP.ORG

Valid starting       Expires              Service principal
01/07/2019 15:01:27  01/08/2019 15:01:27  krbtgt/DEVDIP.ORG@DEVDIP.ORG
        renew until 01/14/2019 15:01:27, Flags: FRI
```

klist -f 票据的标志：

F:可转发

f:已转发

P:可代理

p:代理票据

D:可迟延的票据

d:迟延的票据

R:可更新的票据

I:初始票据

i:无效的票据

H:使用硬件预认证

A：使用预认证

o:服务器是一个代表

klsit-a :显示所有在凭证高速缓存中的票据，包括过期的票据，如果不指定该标志，不列出过期的票据

```
[root@dev-dmp7 bin]# klist -a
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: dmpadmin@DEVDIP.ORG

Valid starting       Expires              Service principal
01/07/2019 15:01:27  01/08/2019 15:01:27  krbtgt/DEVDIP.ORG@DEVDIP.ORG
        renew until 01/14/2019 15:01:27
        Addresses: (none)
```

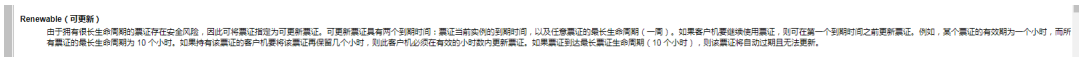
klist -e:显示会话密钥和票据的加密类型

```
[root@dev-dmp7 bin]# klist -e
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: dmpadmin@DEVDIP.ORG

Valid starting       Expires              Service principal
01/07/2019 15:01:27  01/08/2019 15:01:27  krbtgt/DEVDIP.ORG@DEVDIP.ORG
       renew until 01/14/2019 15:01:27, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
```

klsit -l:

```
[root@dev-dmp7 bin]# klist -l
Principal name                 Cache name
--------------                 ----------
dmpadmin@DEVDIP.ORG            FILE:/tmp/krb5cc_0
```


Renewable（可更新）
由于拥有很长生命周期的票证存在安全风险，因此可将票证指定为可更新票证。可更新票证具有两个到期时间：票证当前实例的到期时间，以及任意票证的最长生命周期（一周）。如果客户机要继续使用票证，则可在第一个到期时间之前更新票证。例如，某个票证的有效期为一个小时，而所有票证的最长生命周期为 10 个小时。如果持有该票证的客户机要将该票证再保留几个小时，则此客户机必须在有效的小时数内更新票证。如果票证到达最长票证生命周期（10 个小时），则该票证将自动过期且无法更新。

Renewable（可更新）

由于拥有很长生命周期的票证存在安全风险，因此可将票证指定为可更新票证。可更新票证具有两个到期时间：票证当前实例的到期时间，以及任意票证的最长生命周期（一周）。如果客户机要继续使用票证，则可在第一个到期时间之前更新票证。例如，某个票证的有效期为一个小时，而所有票证的最长生命周期为 10 个小时。如果持有该票证的客户机要将该票证再保留几个小时，则此客户机必须在有效的小时数内更新票证。如果票证到达最长票证生命周期（10 个小时），则该票证将自动过期且无法更新。

总结：

/etc/krb5.conf

```
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 = 62d
 renew_lifetime = 301d
 forwardable = true
 rdns = false
 default_realm = EXPER.ORG
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
  EXPER.ORG = {
   kdc = testdmp1.fengdai.org
   admin_server = testdmp1.fengdai.org
 }

[domain_realm]
  .exper.org = EXPER.ORG
  exper.org = EXPER.ORG
```

ticket_lifetime = 62d

renew_lifetime = 301d

/var/kerberos/krb5kdc/kdc.conf

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

[realms]
 EXPER.ORG = {
  max_life = 91d
  max_renewable_life = 344d
  default_principal_flags = +renewable
  #master_key_type = aes256-cts
  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
 }
```

max_life = 91d

max_renewable_life = 344d

kadmin.local中的krbtgt

```
kadmin.local:  getprinc krbtgt/EXPER.ORG
Principal: krbtgt/EXPER.ORG@EXPER.ORG
Expiration date: [never]
Last password change: [never]
Password expiration date: [never]
Maximum ticket life: 365 days 00:00:00
Maximum renewable life: 364 days 00:00:00
Last modified: Tue Jan 08 10:08:11 CST 2019 (hzpm/admin@EXPER.ORG)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, aes256-cts-hmac-sha1-96
Key: vno 1, aes128-cts-hmac-sha1-96
MKey: vno 1
Attributes: LOCKDOWN_KEYS
Policy: [none]
```

Maximum ticket life: 365 days 00:00:00

Maximum renewable life: 364 days 00:00:00

kadmin.local:hll（自己的prinpical）

```
kadmin.local:  getprinc hll
Principal: hll@EXPER.ORG
Expiration date: [never]
Last password change: Thu Nov 01 14:21:22 CST 2018
Password expiration date: [never]
Maximum ticket life: 300 days 00:00:00
Maximum renewable life: 290 days 00:00:00
Last modified: Tue Jan 08 10:46:02 CST 2019 (root/admin@EXPER.ORG)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 8
Key: vno 1, aes256-cts-hmac-sha1-96
Key: vno 1, aes128-cts-hmac-sha1-96
Key: vno 1, des3-cbc-sha1
Key: vno 1, arcfour-hmac
Key: vno 1, camellia256-cts-cmac
Key: vno 1, camellia128-cts-cmac
Key: vno 1, des-hmac-sha1
Key: vno 1, des-cbc-md5
MKey: vno 1
Attributes:
Policy: [none]
```

Maximum ticket life: 300 days 00:00:00
Maximum renewable life: 290 days 00:00:00

1.对于server端（第一台）：ticket_lifetime和renewable_life的决定因素是下面五个因素中的最小值：
1.1： /etc/krb5.conf中的ticket_lifetime，renew_lifetime
1.2：/var/kerberos/krb5kdc/kdc.conf中的 max_life ，max_renewable_life
1.3：内置的prinpical：krbtgt中的Maximum ticket life, Maximum renewable life
1.4用户自己的prinpical：例hll中的Maximum ticket life, Maximum renewable life
1.5：当前用户下：kinit -l lifetime（5d），kinit -r lifetime(10d) 或者 kinit -l lifetime -r lifetime
ticket_lifetime中的命令参数 :kinit -l lifetime（5d）；
renewable_life中的命令参数：kinit -r lifetime(10d)
指定用户： kinit -l lifetime -r lifetime prinpical 或者kinit -l lifetime prinpical， kinit -r lifetime prinpical

2.对于系统客户端（除第一台之外的其他节点）：ticket_lifetime和renewable_life的决定因素是下面四个因素中的最小值：
2.1： /etc/krb5.conf中的ticket_lifetime，renew_lifetime
2.2：内置的prinpical：krbtgt中的Maximum ticket life, Maximum renewable life

2.3用户自己的prinpical：例hll中的Maximum ticket life，Maximum renewable life

2.4：当前用户下：kinit -l lifetime（5d），kinit -r lifetime(10d) 或者 kinit -l lifetime -r lifetime

ticket_lifetime中的命令参数 :kinit -l lifetime（5d）；

renewable_life中的命令参数：kinit -r lifetime(10d)

指定用户： kinit -l lifetime -r lifetime prinpical 或者kinit -l lifetime prinpical， kinit -r lifetime prinpical

3.windows客户端ticket_lifetime和renewable_life的决定因素是下面四个因素中的最小值：

3.1： Windows上的krb5.ini中的ticket_lifetime，renew_lifetime

3.2：/var/kerberos/krb5kdc/kdc.conf中的 max_life ，max_renewable_life

3.3：内置的prinpical：krbtgt中的Maximum ticket life，Maximum renewable life

3.4用户自己的prinpical：例hll中的Maximum ticket life，Maximum renewable life

4.当重新创建新用户时，prinpical的Maximum ticket life，Maximum renewable life的值的决定因素是/var/kerberos/krb5kdc/kdc.conf中的max_life ，max_renewable_life

5.当使用kinit -l /-r时，只能暂时修改该用户的

ticket_lifetime,renew_lifetime的时间，对kadmin.local中的该用户的Maximum ticket life，Maximum renewable life无影响