Kerberos V5客户端支持的故障排除和配置

目录

简介

本文提供一配置示例，以及一些解决方案给常见问题。帮助您排除故障所有问题的技术在本文也提供。本文不讨论Kerberized Telnet支持。

大多数在附有Kerberos和自多种可用的常见问题的此条款的此材料来自免费可得的文档(常见问题)在包。配置来自一个功能路由器和Kerberos KDC服务器。

本文假设，您正确地编译了并且安装Kerberos包的版本5当前版本从MIT。参考参考在此条款结束时关于如何获取，编译和安装Kerberos的信息V5。

并且请注意Cisco IOS软件版本11.2或以后为Kerberos V5支持要求。Kerberos v客户端验证此提供完全支持，包括证件转发。有Kerberos v基础设施的系统能使用他们的密钥分配分配中心(KDCs)为了验证网络或路由器访问的最终用户。这是客户端实施而不是Kerberos KDC实施。

Kerberos认为传统安全性服务并且是最有利的在已经使用Kerberos的网络。

参考版本包括此支持的Cisco IOS软件版本11.2版本注释欲知更多详细信息。

对于在随后的Cisco IOS软件版本的Kerberos支持，参考软件顾问(仅限注册用户)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS软件版本11.2及以上版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Kerberos 简介

Kerberos是一个网络验证协议为在自然法则上不可靠的网络的使用。Kerberos根据Needham及Schroeder提交的密钥分配型号。(请参阅在本文的References部分的第9。它设计为客户端/服务器应用程序提供强认证使用密钥加密。它允许在网络通信彼此证明他们的标识的实体，当防止窃听或重放攻击时。它也提供数据流完整性(例如修改的检测)和秘密(例如未授权的读的预防)在加密算法系统帮助下例如DES。

用于互联网的许多协议不提供任何安全。用于的工具“探测”密码关闭网络在一般由系统解密高手。因此，发送在未加密的网络的一个密码的应用程序易受攻击。并且，其他客户端/服务器应用程序依靠客户端程序是“诚实的”关于使用它用户的标识。其他应用程序依靠客户端限制其活动到它允许执行的那些，没有其他实施由服务器。

一些站点尝试使用防火墙为了解决他们的网络安全问题。防火墙假设，“坏人”是在外部，经常是一无效假定。然而，造成更多损伤计算机犯罪事件的多数由知情人执行了。防火墙也有一个重大的缺点他们限制您的用户如何能使用互联网。

Kerberos由MIT创建作为对这些网络安全问题的一解决方案。Kerberos协议使用强加密算法，因此客户端能证明其标识到一个服务器(反之亦然)在非安全网络连接间。在客户端和服务器使用Kerberos为了证明他们的标识后，他们能也加密所有他们的通信为了保证保密性和数据完整性，当他们着手他们的事务。

Kerberos从MIT是免费可得，在类似于那个使用BSD操作和X11窗口机制系统的版权权限公告下。MIT提供Kerberos以源程序形式。这执行，以便希望使用它的人能在代码查找为他们自己和保证自己代码值得信任。另外，为在一个支持的产品喜欢专业取决于的那些人， Kerberos是可用的作为从

许多不同的供应商的一种产品。

Kerberos V5客户端支持根据Kerberos认证系统开发在MIT。在Kerberos下，客户端(通常用户或服务)发送一个要求到密钥分配中心(KDC)的一张票。KDC创建赋予票据的票据(TGT)客户端的，在客户端的密码帮助下加密它作为密钥，并且送回已加密TGT到客户端。客户端然后尝试在其密码帮助下解密TGT。如果客户端成功解码例如TGT，如果客户端给正确密码)，保持解密的TGT。这指示客户端的标识的认证。

TGT，在指定时间超时，允许客户端获取另外的票，给特定服务的权限。这些另外的票请求和授予对用户透明的。

因为Kerberos协商已验证，或者加密，并且通信在互联网的任何两个点之间，提供不取决于安全的层防火墙的哪侧任一个客户端查找。Kerberos主要用于应用级协议(ISO型号级别7)，例如Telnet或FTP，为了提供用户主机安全。它也使用，虽然较少频繁地，作为数据流(例如**SOCK_STREAM**)或RPC机制隐式认证系统(ISO模拟级别6)。它可能也使用在更低级的主机对主机安全，在协议例如IP、UDP或者TCP (ISO模拟级别3和4)。虽然，这样实施是少见的，如果他们存在。

它提供相互验证和安全通信负责人之间在开放式网络由密钥制造所有请求方的。也提供通过网络能安全被传播的这些密钥的一机制。Kerberos不提供授权或核算。然而，希望对的应用程序能使用他们的密钥为了安全地执行那些功能。

定义

- **验证**—保证您是谁您说您是，并且我们知道谁您是。
- **客户端**—能获取票的实体。此实体通常是用户或主机。
- **凭证**—同票一样。
- **守护程序**—程序，在UNIX主机运行的通常一个，该服务验证的网络请求。
- **host-a**可以在网络访问的计算机。
- **实例**— Kerberos主管的第二部分。它提供合格主要的信息。实例可以空。一旦用户，实例是常用的为了描述对应的凭证的目标用途。一旦主机，实例是完全合格的主机名。
- **Kerberos** —在希腊神话方面，守卫入口对地狱的三个头的狗。在计算机世界， Kerberos是开发在MIT的网络安全包。
- **KDC** —密钥分配中心。发行Kerberos票的计算机。
- **Keytab** —包含一个或更多密钥的一份关键表文件。主机或服务使用一个Keytab文件，以与用户使用他们的密码相似的方式。
- **NAS** —做TACACS+认证和授权请求的网络接入服务器(思科方框)或别的或者发送核算数据包。
- **首席**—命名一个特定实体一套凭证可以分配的字符串。它通常有三部分名为Primary、实例和领域。一位典型的Kerberos主管的典型的格式是**主要的/instanceREALM**。
- **主要的**— Kerberos主管的第一部分。一旦用户，它是用户名。一旦服务，它是服务的名称。
- **领域**—逻辑网络由单个Kerberos数据库和一套密钥分配分配中心服务。按照惯例，领域名通常是所有大写字母，区分从互联网域的领域。
- **服务**—您在网络访问的任何程序或计算机。服务示例包括：“主机” —主机， (例如，当您使用Telnet和rsh)“ftp” — FTP“krbtgt” —验证;例如赋予票据的票据“pop” —电子邮件
- **票**—验证一个客户端标识特定服务的临时套电子凭证。
- **TGT** —赋予票据的票据。允许客户端获取在同一个Kerberos领域内的另外的Kerberos票的一张特殊Kerberos票。赋予票据的票据的一好类比是好在四种不同的手段的一张三天滑雪通行证。您显示通行证在手段您决定去(直到超时)，并且您接收该手段的一张推力票。一旦有推力票，您能滑雪您希望在该手段的所有。如果去另一种手段次日，您再次显示您的通行证，并且您得到新的手段的一张另外的推力票。差异是Kerberos V5程序注意您有周末滑雪通行证，并且得到您

的推力票，因此您不必须执行处理。

嘿

此部分列出您需要知道的几个项目：

- 确保您取消在配置文件的所有句尾空格。句尾空格能引起问题由于krb5kdc服务器。否则，您能收到说的消息， "krb5kdc不能开始领域的数据库”。
- 确保在路由器的时钟设置为时间和运行KDC服务器的UNIX主机一样。为了防止入侵者重置他们的系统时钟为了继续使用已到期票， Kerberos V5设置拒绝从时钟不在KDC的指定的最大时钟偏移内的所有主机的票请求(在kdc.conf文件上指定)。同样地，主机配置拒绝从时钟不在主机的指定的最大时钟偏移内的所有KDC的答复(在krb5.conf文件上指定)。最大时钟不对称性的默认值是300秒(五分钟)。
- 适当地确保DNS工作。Kerberos的几个方面依靠名称服务。为了Kerberos能提供其高级安全设施，它对名称服务问题比您的网络的一些其他部分是敏感。重要的是您的域名系统(DNS)条目和您的主机有正确信息。每规范主机名必须是包括域)的完全合格的主机名(，并且主机的每个IP地址必须负面解析到规范名。
- Cisco IOS Kerberos V5支持不允许使用小写领域名称，并且在Cisco IOS的Kerberos代码不验证用户，如果领域用小写。这在Cisco IOS软件版本11.2(7)修复。参考的Cisco Bug ID CSCdj10598 (仅限注册用户)。唯一的应急方案是使用(是常规的)的大写领域名。小写领域工作为了获取TGT，但是不是服务凭证。因为思科使用他们新的TGT为了在记录日志验证时获取服务凭证(用于防止KDC欺骗攻击)，使用小写领域的Kerberos认证总是发生故障。
- PPP PAP和CHAP的Kerberos V5能失败路由器。这在Cisco IOS软件版本11.2(6)修复。参考的Cisco Bug ID CSCdj08828 (仅限注册用户)。此的应急方案是强制EXEC登录到路由器通过**异步模式交互**没有**自动选择在登录期间**手工然后有用户启动PPP ：`aaa authentication ppp default if-needed krb5 local`
- Kerberos V5不执行授权或核算。您需要某个其他代码为了执行此。

Cisco IOS路由器配置

在此部分的配置表示执行Kerberos V5的一个充分地已配置的AS5200路由器。路由器在此配置方面使用Kerberos服务器为了验证拨号执行与PAP认证的PPP的VTY会话和用户。

与Kerberos V5的AS5200设置

```
version 11.2
service timestamps debug datetime msec
!
hostname cisco5200
!
aaa new-model
aaa authentication login cisco2 krb5 local
aaa authentication ppp cisco krb5 local
enable secret
enable password
!
username cisco password cisco
ip host-routing
ip domain-name cisco.edu
ip name-server 10.10.1.25
ip name-server 10.10.20.3
kerberos local-realm CISCO.EDU
```

```
kerberos srvtab entry host/cisco5200.cisco.edu@CISCO.EDU
0 861289666 2
1 80:>:11338>531159=
!
 !--- You do not actually enter the previous line. !---
Enter "kerberos srvtab remote 10.10.1.8 /ts/krb5.keytab"
and the !--- the router TFTPs the key entry on its own.
kerberos server CISCO.EDU 10.10.1.8 kerberos credentials
forward isdn switch-type primary-5ess clock timezone GMT
-6 clock summer-time CDT recurring ! controller T1 0
framing esf clock source line primary linecode b8zs pri-
group timeslots 1-24 ! controller T1 1 framing esf clock
source line secondary linecode b8zs pri-group timeslots
1-24 ! interface Ethernet0 ip address 10.10.110.245
255.255.255.0 no ip mroute-cache ! interface Serial0 no
ip address no ip mroute-cache shutdown ! interface
Serial1 no ip address no ip mroute-cache shutdown !
interface Serial0:23 ip unnumbered Ethernet0 no ip
mroute-cache encapsulation ppp isdn incoming-voice modem
no cdp enable ! interface Serial1:23 ip unnumbered
Ethernet0 no ip mroute-cache encapsulation ppp isdn
incoming-voice modem no cdp enable ! interface Group-
Async1 ip unnumbered Ethernet0 no ip mroute-cache
encapsulation ppp async mode interactive peer default ip
address pool mypool dialer in-band dialer idle-timeout
9999 dialer-group 1 no cdp enable ppp authentication pap
cisco group-range 1 48 ! ip local pool mypool
10.10.110.97 10.10.110.144 no ip classless ip route
0.0.0.0 0.0.0.0 10.10.110.254 ! dialer-list 1 protocol
ip permit ! line con 0 login authentication test line 1
48 autoselect ppp login authentication cisco2 modem
InOut transport input all line aux 0 modem InOut
transport input all flowcontrol hardware line vty 0 10
exec-timeout 0 0 login authentication cisco2 ! end
```

Kerberos KDC配置

确保您有为**inetd**设置的适当的端口。

注意： 此示例使用封皮。如果想要已加密Telnet，您需要用Kerberized Telnet替换正常Telnet，因此这些文件有一不同的外观。

inetd的设置端口

```
# cat /etc/services
-----------------------------------------------------------------
#
# Syntax:  ServiceName PortNumber/ProtocolName [alias\_1,...,alias\_n] [#comments]
#
# ServiceNameofficial Internet service name
# PortNumber the socket port number used for the service
# ProtocolNamethe transport protocol used for the service
# alias                 unofficial service names
# #comments             text following the comment character (#) is ignored
#
tftp69/udp

kerberos88/udpkdc
kerberos88/tcpkdc
```

```
kxct549/tcp

klogin      543/tcp         # Kerberos authenticated rlogin
kshell 544/tcp         cmd # and remote shell
kerberos-adm 749/tcp          # Kerberos 5 admin/changepw
kerberos-adm 749/udp        # Kerberos 5 admin/changepw
kerberos-sec 750/udp         kdc    # Kerberos authentication--udp
kerberos-sec   750/tcp         kdc   # Kerberos authentication--tcp
krb5\_prop    754/tcp          # Kerberos slave propagation
eklogin       2105/tcp         # Kerberos auth. & encrypted rlogin
krb524        4444/tcp         # Kerberos 5 to 4 ticket translator
-----------------------------------------------------------------

#cat /etc/inetd.conf

ident   stream  tcp     nowait  root    /usr/local/etc/in.identd in.identd
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd          ftpd
telnet  stream  tcp     nowait  root    /usr/sbin/tcpd          telnetd
#shell   stream  tcp     nowait  root    /usr/sbin/tcpd          rshd
shell   stream  tcp     nowait  root    /usr/sbin/rshd          rshd
#login   stream  tcp     nowait  root    /usr/sbin/tcpd          rlogind
login   stream  tcp     nowait  root    /usr/sbin/rlogind       rlogind
exec    stream  tcp     nowait  root    /usr/sbin/rexecd        rexecd
# Run as user "uucp" if you don't want uucpd's wtmp entries.
#uucp   stream  tcp     nowait  root    /usr/sbin/uucpd         uucpd
#finger  stream  tcp     nowait  root    /usr/sbin/tcpd          fingerd
# tftp was /tmp and is now /ts for terminal server macros
tftp    dgram   udp     wait    nobody  /usr/sbin/tcpd          tftpd /ts
comsat  dgram   udp     wait    root    /usr/sbin/comsat        comsat
-----------------------------------------------------------------
```

设置Kerberos配置文件

其次，您需要设置KDC服务器读的一些个Kerberos配置文件。关于什么的更多信息这些参数含义，参考Kerberos安装指南或系统管理员指南 。

```
# cat /etc/krb5.conf

[libdefaults]
        default_realm =  CISCO.EDU
        ticket_lifetime = 600
        default_tgs_enctypes = des-cbc-crc
        default_tkt_enctypes = des-cbc-crc

[realms]
        CISCO.EDU = {
        kdc =  ciscoaxa.cisco.edu:88
        admin_server =  ciscoaxa.cisco.edu
        default_domain =  CISCO.EDU
        }

[domain_realm]
        .cisco.edu = CISCO.EDU
        cisco.edu  = CISCO.EDU

[logging]
        kdc = FILE:/var/log/krb5kdc.log
        admin_server = FILE:/var/log/kadmin.log
        default = FILE:/var/log/krb5lib.log


# cat /usr/local/var/krb5kdc/kdc.conf
```

```
[kdcdefaults]
      kdc_ports = 88,750

[realms]
      CISCO.EDU = {
         database_name = /usr/local/var/krb5kdc/principal
         admin_keytab = FILE:/usr/local/var/krb5kdc/kadm5.keytab
         acl_file = /usr/local/var/krb5kdc/kadm5.acl
         acl_file = /usr/local/var/krb5kdc/kadm5.dict
         key_stash_file = /usr/local/var/krb5kdc/.k5.CISCO.EDU
         kadmind_port = 749
         max_life = 10h 0m 0s
         max_renewable_life = 7d 0h 0m 0s
         master_key_type = des-cbc-crc
         supported_enctypes = des-cbc-crc:normal des:normal des:v4
des:norealm des:onlyrealm des:afs3
     }
```

设置KDC服务器的数据库

其次，您需要创建KDC服务器使用的数据库。

1. 输入kdb5_util命令：`# kadmin/dbutil/kdb5_util Usage: kdb5_util cmd [-r realm] [-d dbname] [-k mkeytype] [-M mkeyname] [-m] [cmd options] create [-s] destroy [-f] stash [-f keyfile] dump [-old] [-ov] [-b6] [-verbose] [filename [princs...]] load [-old] [-ov] [-b6] [-verbose] [-update] filename dump_v4 [filename] load_v4 [-t] [-n] [-v] [-K] [-s stashfile] inputfile ---------- # kadmin/dbutil/kdb5_util destroy -r cisco.edu kdb5_util: No such file or directory while setting active database to "/usr/local/var/krb5kdc/principal" # kadmin/dbutil/kdb5_util create -r CISCO.EDU -s Initializing database '/usr/local/var/krb5kdc/principal' for realm 'CISCO.EDU', master key name 'K/M@CISCO.EDU' 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:` 这是需要的为了从路由器检索srvtab密码通过TFTP用kerberos srvtab remote命令。`# kadmin/dbutil/kdb5_util stash -r CISCO.EDU Enter KDC database master key:`
2. 为了添加负责人和用户到数据库，请使用kadmin.local命令：`# kadmin/cli/kadmin.local kadmin.local: listprincs kadmin/admin@CISCO.EDU kadmin/changepw@CISCO.EDU K/M@CISCO.EDU krbtgt/CISCO.EDU@CISCO.EDU kadmin/history@CISCO.EDU kadmin.local: kadmin.local: ? Available kadmin.local requests: add_principal, addprinc, ank Add principal delete_principal, delprinc Delete principal modify_principal, modprinc Modify 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 list_requests, lr, ? List available requests. quit, exit, q Exit program. ---------- ------------------------------`
3. 添加一个用户：`kadmin.local:  ank cisco1@CISCO.EDU`
   `Enter password for principal "cisco1@CISCO.EDU":`
   `Re-enter password for principal "cisco1@CISCO.EDU":`
   `Principal "cisco1@CISCO.EDU" created.`
4. 得到当前数据库的列表：`kadmin.local:  listprincs`
   `kadmin/admin@CISCO.EDU`
   `kadmin/changepw@CISCO.EDU`
   `cisco1@CISCO.EDU`
   `K/M@CISCO.EDU`
   `krbtgt/CISCO.EDU@CISCO.EDU`
   `kadmin/history@CISCO.EDU`
5. 添加Cisco路由器的条目：`kadmin.local:  ank host/cisco5200.cisco.edu@CISCO.EDU`
   `Enter password for principal "host/cisco5200.cisco.edu@CISCO.EDU":`

```
Re-enter password for principal "host/cisco5200.cisco.edu@CISCO.EDU":
Principal "host/cisco5200.cisco.edu@CISCO.EDU" created.
```

6. 解压缩密钥对Cisco路由器的表：`kadmin.local:  ktadd host/cisco5200.cisco.edu@CISCO.EDU`
   ```
   Entry for principal host/cisco5200.cisco.edu@CISCO.EDU with kvno 2,
      encryption type DES-CBC-CRC added to keytab WRFILE:/etc/krb5.keytab.
   ```
7. 看一看在数据库：`kadmin.local:  listprincs`
   ```
   kadmin/admin@CISCO.EDU
   kadmin/changepw@CISCO.EDU
   cisco1@CISCO.EDU
   K/M@CISCO.EDU
   krbtgt/CISCO.EDU@CISCO.EDU
   kadmin/history@CISCO.EDU
   host/cisco5200.cisco.edu@CISCO.EDU

   kadmin.local:  quit
   ```
8. 搬到Keytab文件路由器能达到它的地方：`# cp /etc/krb5.keytab /ts/`
   `# chmod 777 /ts/krb5.keytab`
9. 启动KDC服务器：`# kdc/krb5kdc`
   `#`
10. 检查确保它实际上运行：`# ps -A | grep  'krb5'`
    ```
     6043 ??       I        0:00.01 kdc/krb5kdc
    23427 ttypf    S  +     0:00.05 grep krb5
    ```
11. 强制路由器读其关键条目：`cisco5200(config)#`**`kerberos srvtab remote 10.10.1.8 /ts/krb5.keytab`** `Loading /ts/krb5.keytab from 10.10.1.8 (via Ethernet0): ! [OK - 229/1000 bytes]`
12. 检查路由器确保一切准备好：`cisco5200#`**`write terminal`** `aaa new-model aaa authentication login cisco2 krb5 local aaa authentication ppp cisco krb5 local kerberos local-realm CISCO.EDU kerberos srvtab entry host/cisco5200.cisco.edu@CISCO.EDU 0 861289666 2 1 8 0:>:11338>531159= kerberos server CISCO.EDU 10.10.1.8 kerberos credentials forward`
13. 启用调试并且设法登录路由器：`cisco5200#`**`terminal monitor`** `cisco5200#`**`debug kerberos`** `Kerberos debugging is on cisco5200#`**`debug aaa authen`** `AAA Authentication debugging is on cisco5200#`**`show clock`** `10:16:41.797 CDT Thu Apr 17 1997 cisco5200# Apr 17 15:16:58.965: AAA/AUTHEN: create_user user='' ruser='' port='tty51' rem_addr='12.12.109.64' authen_TYPE=ASCII service=LOGIN priv=1 Apr 17 15:16:58.969: AAA/AUTHEN/START (0): port='tty51' list='cisco2' ACTION=LOGIN service=LOGIN Apr 17 15:16:58.969: AAA/AUTHEN/START (1957396): found list Apr 17 15:16:58.973: AAA/AUTHEN/START (1667706374): METHOD=KRB5 Apr 17 15:16:58.973: AAA/AUTHEN (1667706374): status = GETUSER Apr 17 15:17:02.493: AAA/AUTHEN/CONT (1667706374): continue_login Apr 17 15:17:02.493: AAA/AUTHEN (1667706374): status = GETUSER Apr 17 15:17:02.497: AAA/AUTHEN (1667706374): METHOD=KRB5 Apr 17 15:17:02.497: AAA/AUTHEN (1667706374): status = GETPASS Apr 17 15:17:05.401: AAA/AUTHEN/CONT (1667706374): continue_login Apr 17 15:17:05.405: AAA/AUTHEN (1667706374): status = GETPASS Apr 17 15:17:05.405: AAA/AUTHEN (1667706374): METHOD=KRB5 Apr 17 15:17:05.413: Kerberos: Requesting TGT with expiration date of 861319025 Apr 17 15:17:05.417: Kerberos: Sending TGT request with no pre-authorization data. Apr 17 15:17:05.441: Kerberos: Sent TGT request to KDC Apr 17 15:17:06.405: Kerberos: Received TGT reply from KDC Apr 17 15:17:06.465: Domain: query for 245.110.10.10.in-addr.arpa to 10.10.1.25 Reply received ok Apr 17 15:17:06.569: Kerberos: Sent TGT request to KDC Apr 17 15:17:06.769: Kerberos: Received TGT reply from KDC Apr 17 15:17:06.881: Kerberos: Received valid credential with endtime of 861232625 Apr 17 15:17:06.897: AAA/AUTHEN (1667706374): status = PASS`

调试输出示例

这是成功验证的PPP用户。

`cisco5200#`**`debug ppp auth`** `Apr 17 15:47:15.285: Async6: Dialer received incoming call from <unknown> %LINK-3-UPDOWN: Interface Async6, changed state to up Apr 17 15:47:17.293: Async6: Dialer received incoming call from <unknown> Apr 17 15:47:17.909: PPP Async6: PAP receive authenticate request cisco1 Apr 17 15:47:17.913: PPP Async6: PAP authenticating peer cisco1 Apr`

```
17 15:47:17.917: AAA/AUTHEN: create_user user='cisco1' ruser='' port='Async6'
rem_addr='async/6151010' authen_TYPE=PAP service=PPP priv=1 Apr 17 15:47:17.917:
AAA/AUTHEN/START (0): port='Async6' list='cisco' ACTION=LOGIN service=PPP Apr 17 15:47:17.921:
AAA/AUTHEN/START (4706358): found list Apr 17 15:47:17.921: AAA/AUTHEN/START (712179591):
METHOD=KRB5 Apr 17 15:47:17.929: Kerberos: Requesting TGT with expiration date of 861320837 Apr
17 15:47:17.933: Kerberos: Sending TGT request with no pre-authorization data. Apr 17
15:47:17.957: Kerberos: Sent TGT request to KDC Apr 17 15:47:18.765: Kerberos: Received TGT
reply from KDC Apr 17 15:47:18.893: Kerberos: Sent TGT request to KDC Apr 17 15:47:19.097:
Kerberos: Received TGT reply from KDC Apr 17 15:47:19.205: Kerberos: Received valid credential
with endtime of 861234437 Apr 17 15:47:19.221: AAA/AUTHEN (712179591): status = PASS Apr 17
15:47:19.225: PPP Async6: Remote passed PAP authentication sending Auth-Ack. Apr 17
15:47:19.225: Async6: authenticated host cisco1 with no matching dialer map %LINEPROTO-5-UPDOWN:
Line protocol on Interface Async6, changed state to up
```

故障排除

此部分包含潜在问题的多种方案。这些调试帮助您迅速发现问题。

错误的领域名

```
cisco5200#
cisco5200#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
cisco5200(config)#kerberos local-realm junk.COM cisco5200# Apr 17 15:19:16.089: AAA/AUTHEN:
create_user user='' ruser='' port='tty51' rem_addr='12.12.109.64' authen_TYPE=ASCII
service=LOGIN priv=1 Apr 17 15:19:16.093: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
ACTION=LOGIN service=LOGIN Apr 17 15:19:16.097: AAA/AUTHEN/START (1957396): found list Apr 17
15:19:16.129: AAA/AUTHEN/START (56280416): METHOD=KRB5 Apr 17 15:19:16.129: AAA/AUTHEN
(56280416): status = GETUSER Apr 17 15:19:21.721: AAA/AUTHEN/CONT (56280416): continue_login Apr
17 15:19:21.721: AAA/AUTHEN (56280416): status = GETUSER Apr 17 15:19:21.725: AAA/AUTHEN
(56280416): METHOD=KRB5 Apr 17 15:19:21.725: AAA/AUTHEN (56280416): status = GETPASS Apr 17
15:19:26.057: AAA/AUTHEN/CONT (56280416): continue_login Apr 17 15:19:26.057: AAA/AUTHEN
(56280416): status = GETPASS Apr 17 15:19:26.061: AAA/AUTHEN (56280416): METHOD=KRB5 Apr 17
15:19:26.065: Kerberos: Requesting TGT with expiration date of 861319166 Apr 17 15:19:26.069:
Kerberos: Sending TGT request with no pre-authorization data. Apr 17 15:19:26.089: Kerberos:
Received invalid credential. ~~~~~~~~~~~~~~~~~~ Apr 17 15:19:26.093: AAA/AUTHEN (56280416):
password incorrect Apr 17 15:19:26.097: AAA/AUTHEN (56280416): status = FAIL Apr 17
15:19:28.169: AAA/AUTHEN: free user cisco1 tty51 12.12.109.64 authen_TYPE=ASCII service=LOGIN
priv=1 Apr 17 15:19:28.173: AAA/AUTHEN: create_user user='' ruser='' port='tty51'
rem_addr='12.12.109.64' authen_TYPE=ASCII service=LOGIN priv=1 Apr 17 15:19:28.177:
AAA/AUTHEN/START (0): port='tty51' list='cisco2' ACTION=LOGIN service=LOGIN Apr 17 15:19:28.177:
AAA/AUTHEN/START (1957396): found list Apr 17 15:19:28.181: AAA/AUTHEN/START (126312328):
METHOD=KRB5 Apr 17 15:19:28.181: AAA/AUTHEN (126312328): status = GETUSER
```

DNS不工作

```
Apr 10 17:22:15.370: Kerberos:  Requesting TGT with expiration date
    of 860721735
Apr 10 17:22:15.374: Kerberos:  Sending TGT request with no
pre-authorization data.
Apr 10 17:22:15.398: Kerberos:  Sent TGT request to KDC
Apr 10 17:22:16.034: Kerberos:  Received TGT reply from KDC
Apr 10 17:22:16.090: Domain: query for 245.110.10.10.in-addr.arpa
        to 255.255.255.255 Reply received empty
                                          ~~~~
```

不正确的路由器时钟

```
pppcisco1#
Apr 18 20:41:41.011: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
```

```
Apr 18 20:41:41.011: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 20:41:41.015: AAA/AUTHEN/START (1957396): found list
Apr 18 20:41:41.015: AAA/AUTHEN/START (4036314657): METHOD=KRB5
Apr 18 20:41:41.019: AAA/AUTHEN (4036314657): status = GETUSER
Apr 18 20:41:43.835: AAA/AUTHEN/CONT (4036314657): continue_login
Apr 18 20:41:43.839: AAA/AUTHEN (4036314657): status = GETUSER
Apr 18 20:41:43.839: AAA/AUTHEN (4036314657): METHOD=KRB5
Apr 18 20:41:43.843: AAA/AUTHEN (4036314657): status = GETPASS
Apr 18 20:41:48.835: AAA/AUTHEN/CONT (4036314657): continue_login
Apr 18 20:41:48.839: AAA/AUTHEN (4036314657): status = GETPASS
Apr 18 20:41:48.839: AAA/AUTHEN (4036314657): METHOD=KRB5
Apr 18 20:41:48.847: Kerberos:  Requesting TGT with expiration date
     of 861424908
Apr 18 20:41:48.851: Kerberos:  Sending TGT request with no
     pre-authorization data.
Apr 18 20:41:48.875: Kerberos:  Sent TGT request to KDC
Apr 18 20:41:49.675: Kerberos:  Received TGT reply from KDC
Apr 18 20:41:49.795: Kerberos:  Sent TGT request to KDC
Apr 18 20:41:50.119: Kerberos:  Received TGT reply from KDC
Apr 18 20:41:50.155: AAA/AUTHEN (4036314657): password incorrect
Apr 18 20:41:50.159: AAA/AUTHEN (4036314657): status = FAIL
Apr 18 20:41:52.235: AAA/AUTHEN: free user cisco1  tty51 171.68.109.64
                     authen_TYPE=ASCII service=LOGIN priv=1
Apr 18 20:41:52.239: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 20:41:52.243: AAA/AUTHEN/START (0): port='tty51' list='cisco2' A
     CTION=LOGIN service=LOGIN
Apr 18 20:41:52.243: AAA/AUTHEN/START (1957396): found list
Apr 18 20:41:52.247: AAA/AUTHEN/START (1817975874): METHOD=KRB5
Apr 18 20:41:52.247: AAA/AUTHEN (1817975874): status = GETUSER
Apr 18 20:42:08.143: AAA/AUTHEN/ABORT: (1817975874) because
     Carrier dropped.
Apr 18 20:42:08.147: AAA/AUTHEN: free user   tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
----------------------
```

这是什么用户看到：

```
$telnet 10.10.110.245 Trying 10.10.110.245 ... Connected to 10.10.110.245. Escape character is
'^]'. User Access Verification Username: cisco1 Password: Kerberos: Failed to retrieve temporary
service credentials! Kerberos: Failed to validate TGT! % Access denied Username:
```

客户端不Kerberos数据库的

```
Apr 18 19:04:49.983: AAA/AUTHEN: create_user user=''
     ruser='' port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:04:49.987: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:04:49.987: AAA/AUTHEN/START (1957396): found list
Apr 18 19:04:49.991: AAA/AUTHEN/START (3962282505): METHOD=KRB5
Apr 18 19:04:49.995: AAA/AUTHEN (3962282505): status = GETUSER
Apr 18 19:04:53.475: AAA/AUTHEN/CONT (3962282505): continue_login
Apr 18 19:04:53.479: AAA/AUTHEN (3962282505): status = GETUSER
Apr 18 19:04:53.479: AAA/AUTHEN (3962282505): METHOD=KRB5
Apr 18 19:04:53.483: AAA/AUTHEN (3962282505): status = GETPASS
Apr 18 19:04:56.283: AAA/AUTHEN/CONT (3962282505): continue_login
Apr 18 19:04:56.283: AAA/AUTHEN (3962282505): status = GETPASS
Apr 18 19:04:56.287: AAA/AUTHEN (3962282505): METHOD=KRB5
Apr 18 19:04:56.291: Kerberos:  Requesting TGT with expiration date
     of 861419096
Apr 18 19:04:56.295: Kerberos:  Sending TGT request with no
```

```
     pre-authorization data.
Apr 18 19:04:56.323: Kerberos:  Sent TGT request to KDC
Apr 18 19:04:56.355: Kerberos:  Received TGT reply from KDC
Apr 18 19:04:56.363: Kerberos:  Client not found in Kerberos database
                                ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Apr 18 19:04:56.371: Kerberos:  Received invalid credential.
Apr 18 19:04:56.375: AAA/AUTHEN (3962282505): password incorrect
Apr 18 19:04:56.379: AAA/AUTHEN (3962282505): status = FAIL
Apr 18 19:04:58.679: AAA/AUTHEN: free user cisco3  tty51 171.68.109.64
                         authen_TYPE=ASCII service=LOGIN priv=1
Apr 18 19:04:58.687: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:04:58.687: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:04:58.691: AAA/AUTHEN/START (1957396): found list
Apr 18 19:04:58.743: AAA/AUTHEN/START (1209738018): METHOD=KRB5
Apr 18 19:04:58.747: AAA/AUTHEN (1209738018): status = GETUSER
Apr 18 19:05:04.863: AAA/AUTHEN/ABORT: (1209738018) because
     Carrier dropped.
Apr 18 19:05:04.863: AAA/AUTHEN: free user   tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
```

客户端是在数据库，但是用途错误的密码

```
Apr 18 19:06:05.427: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:06:05.427: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:06:05.431: AAA/AUTHEN/START (1957396): found list
Apr 18 19:06:05.431: AAA/AUTHEN/START (3693437965): METHOD=KRB5
Apr 18 19:06:05.435: AAA/AUTHEN (3693437965): status = GETUSER
Apr 18 19:06:07.763: AAA/AUTHEN/CONT (3693437965): continue_login
Apr 18 19:06:07.763: AAA/AUTHEN (3693437965): status = GETUSER
Apr 18 19:06:07.767: AAA/AUTHEN (3693437965): METHOD=KRB5
Apr 18 19:06:07.767: AAA/AUTHEN (3693437965): status = GETPASS
Apr 18 19:06:14.895: AAA/AUTHEN/CONT (3693437965): continue_login
Apr 18 19:06:14.899: AAA/AUTHEN (3693437965): status = GETPASS
Apr 18 19:06:14.899: AAA/AUTHEN (3693437965): METHOD=KRB5
Apr 18 19:06:14.907: Kerberos:  Requesting TGT with expiration date
     of 861419174
Apr 18 19:06:14.907: Kerberos:  Sending TGT request with no
     pre-authorization data.
Apr 18 19:06:14.935: Kerberos:  Sent TGT request to KDC
Apr 18 19:06:15.643: Kerberos:  Received TGT reply from KDC
Apr 18 19:06:15.683: Kerberos:  Received invalid credential.
Apr 18 19:06:15.687: AAA/AUTHEN (3693437965): password incorrect
                                              ~~~~~~~~~~~~~~~~~~
Apr 18 19:06:15.691: AAA/AUTHEN (3693437965): status = FAIL
Apr 18 19:06:17.695: AAA/AUTHEN: free user cisco1  tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
Apr 18 19:06:17.699: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:06:17.703: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:06:17.703: AAA/AUTHEN/START (1957396): found list
Apr 18 19:06:17.707: AAA/AUTHEN/START (1568599595): METHOD=KRB5
Apr 18 19:06:17.707: AAA/AUTHEN (1568599595): status = GETUSER
Apr 18 19:06:22.751: AAA/AUTHEN/ABORT: (1568599595) because
     Carrier dropped.
Apr 18 19:06:22.755: AAA/AUTHEN: free user   tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
```

用户看到此输出：

```
Trying 10.10.110.245 ...
Connected to 10.10.110.245.
Escape character is '^]'.


User Access Verification

Username: cisco1 Password: % Access denied Username:
```

SRVTAB条目不正确在路由器

```
pppcisco1#
%SYS-5-CONFIG_I: Configured from console by vty0 (171.68.109.64)
Apr 18 19:08:55.799: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:08:55.803: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:08:55.807: AAA/AUTHEN/START (1957396): found list
Apr 18 19:08:55.807: AAA/AUTHEN/START (3369934519): METHOD=KRB5
Apr 18 19:08:55.811: AAA/AUTHEN (3369934519): status = GETUSER
Apr 18 19:08:59.011: AAA/AUTHEN/CONT (3369934519): continue_login
Apr 18 19:08:59.011: AAA/AUTHEN (3369934519): status = GETUSER
Apr 18 19:08:59.015: AAA/AUTHEN (3369934519): METHOD=KRB5
Apr 18 19:08:59.015: AAA/AUTHEN (3369934519): status = GETPASS
Apr 18 19:09:02.219: AAA/AUTHEN/CONT (3369934519): continue_login
Apr 18 19:09:02.219: AAA/AUTHEN (3369934519): status = GETPASS
Apr 18 19:09:02.223: AAA/AUTHEN (3369934519): METHOD=KRB5
Apr 18 19:09:02.231: Kerberos:  Requesting TGT with expiration date
     of 861419342
Apr 18 19:09:02.231: Kerberos:  Sending TGT request with no
     pre-authorization data.
Apr 18 19:09:02.259: Kerberos:  Sent TGT request to KDC
Apr 18 19:09:02.311: Kerberos:  Received TGT reply from KDC
Apr 18 19:09:02.435: Kerberos:  Sent TGT request to KDC
Apr 18 19:09:02.555: Kerberos:  Received TGT reply from KDC
Apr 18 19:09:02.643: AAA/AUTHEN (3369934519): password incorrect
Apr 18 19:09:02.643: AAA/AUTHEN (3369934519): status = FAIL
Apr 18 19:09:04.779: AAA/AUTHEN: free user cisco1  tty51 171.68.109.64
                     authen_TYPE=ASCII service=LOGIN priv=1
Apr 18 19:09:04.783: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:09:04.787: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:09:04.791: AAA/AUTHEN/START (1957396): found list
Apr 18 19:09:04.843: AAA/AUTHEN/START (2592922252): METHOD=KRB5
Apr 18 19:09:04.843: AAA/AUTHEN (2592922252): status = GETUSER
Apr 18 19:09:11.751: AAA/AUTHEN/ABORT: (2592922252) because
     Carrier dropped.
Apr 18 19:09:11.755: AAA/AUTHEN: free user   tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
```

这是什么用户看到：

```
Trying 10.10.110.245 ...
Connected to 10.10.110.245.
Escape character is '^]'.


User Access Verification
```

```
Username: cisco1 Password: Failed to retrieve SRVTAB key! Kerberos: Failed to validate TGT! %
Access denied Username:
```

参考

1. Kerberos V5*系统管理员的指南*(进来一个涂焦油， G-zip压缩的文件)
2. Kerberos V5*安装指南*
3. Kerberos V5 *UNIX用户指南*
4. Kerberos ：网络验证协议
5. Kerberos网络验证服务(USC/ISI's GOST组)
6. Jennifer G. Steiner， Clifford Neuman， Jeffrey I. Schiller。“Kerberos ：开放网络系统的一验证服务”， USENIX 1988年3月
7. S. P. Miller、B.C. Neuman， J.I. Schiller和J.H. Saltzer、“Kerberos认证和授权系统”， 12/21/87
8. R. M. Needham和M.D.施罗德， “使用验证的加密在计算机大型网络”， ACM的通信，第21(12)卷，页。993-999 (December， 1978)
9. V. I. Voydock和S.T.肯特， “在高级网络协议的安全机制”， *Computing Surveys*，第15(2)卷，ACM (六月1983)
10. Li Gong，“根据同步的时钟安全风险”，*操作系统复核*，第26卷， #1，页49-53
11. C. Neuman和J.科尔， “Kerberos网络验证服务(V5)," RFC 1510，九月1993年
12. B. Clifford Neuman和西奥多Ts'o， “Kerberos ：计算机网络的一验证服务”， IEEE通信，32(9)，九月1994年**注意：** 许多这些文档，那由Neuman包括那个， Schiller，并且Steiner (#9)通过从MIT阿西纳系统的FTP也是可用的--Kerberos文档 。为了得到RFC的复制，参考获取的RFC和标准文档。

相关信息

- Kerberos 支持页
- 技术支持 - Cisco Systems