Kerberos V5客户端支持的故障排除和配置

目录

简介

本文档提供了一个配置示例，以及一些常见问题的解决方案。本文档还提供有助于您排除任何问题的技术。本文档不提供核心化Telnet支持。

本文中的大部分内容来自Kerberos随附的免费可用文档以及软件包中各种常见问题(FAQ)。配置来自功能正常的路由器和Kerberos KDC服务器。

本文档假设您已正确编译并安装了来自MIT的Kerberos软件包的第5版。有关如何获取、编译和安装Kerberos V5的信息，请参阅本文末尾的参考资料。

另请注意，Kerberos V5支持需要Cisco IOS®软件版本11.2或更高版本。这提供了对Kerberos V客户端身份验证的完全支持，包括凭证转发。具有Kerberos V基础设施的系统可以使用其密钥分发中心(KDC)对最终用户进行网络或路由器访问身份验证。这是客户端实现，而不是Kerberos KDC实现。

Kerberos被视为一种传统安全服务，在已经使用Kerberos的网络中最有益。

有关包含此支持的版本的更多详细信息，请参阅Cisco IOS软件版本11.2。

有关后续Cisco IOS软件版本中的Kerberos支持，请参阅软件顾问(仅限注册客户)。

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及更高版本

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

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

Kerberos 简介

Kerberos是一种网络身份验证协议，用于物理上不安全的网络。Kerberos基于Needham和Schroeder提出的密钥分配模型。(请参阅本文档“参考”部分的第9号。它旨在通过使用密钥加密为客户端/服务器应用提供强身份验证。它允许通过网络通信的实体在防止窃听或重播攻击的同时，向彼此证明其身份。它还借助DES等加密系统提供数据流完整性（如修改检测）和保密性（如防止未授权读取）。

Internet中使用的许多协议都不提供任何安全性。用于“嗅探”网络密码的工具是系统破解程序的常用工具。因此，通过网络发送口令的应用程序会受到攻击。此外，其他客户端/服务器应用程序依赖客户端程序来“诚实”地了解使用它的用户的身份。其他应用程序依赖客户端将其活动限制为允许其执行的活动，而服务器不执行其他任务。

一些站点尝试使用防火墙来解决其网络安全问题。防火墙假定“坏人”是外部人，这通常是一个无效的假设。但是，造成更大损害的计算机犯罪事件中，大多数是由内部人士实施的。防火墙还有一个显着的缺点，即它们限制了用户使用Internet的方式。

Kerberos是MIT创建的，用于解决这些网络安全问题。Kerberos协议使用强加密，因此客户端可以通过不安全的网络连接向服务器证明其身份（反之亦然）。在客户端和服务器使用Kerberos来证明其身份后，他们还可以加密其所有通信，以确保在业务过程中的隐私和数据完整性。

Kerberos可从MIT免费获得，版权许可通知与BSD操作和X11窗口系统使用的版权许可通知类似。MIT以源形式提供Kerberos。这样，任何希望使用该代码的人都可以自己查看代码，并确保代码可信。此外，对于那些希望依赖专业支持产品的用户，Kerberos可作为来自许多不同供应商的产品提供。

Kerberos V5客户端支持基于MIT开发的Kerberos身份验证系统。在Kerberos下，客户端（通常是用户或服务）向密钥分发中心(KDC)发送票证请求。 KDC为客户端创建票证授予票证(TGT)，借助客户端的密码将其加密为密钥，并将加密的TGT发送回客户端。然后，客户端尝试在其密码的帮助下解密TGT。如果客户端成功解密TGT（例如，如果客户端提供正确的密码），则它保留已解密的TGT。这表示客户端身份的证明。

TGT在指定时间到期，允许客户端获取额外票证，从而授予特定服务的权限。这些额外票证的请求和授权是用户透明的。

由于Kerberos会协商身份验证、可选地加密，并在Internet上的任意两个点之间通信，因此它提供的安全层不依赖于客户端和防火墙的哪一端。Kerberos主要用于应用级协议（ISO模型第7级），如Telnet或FTP，以便为用户提供主机安全。它也作为数据流的隐式身份验证系统（如SOCK_STREAM）或RPC机制（ISO模型级别6）使用，但使用频率较低。 它也可用于较低级别的主机到主机安全，在IP、UDP或TCP（ISO模型第3级和第4级）等协议中。 尽管如此，这种实施非常罕见，如果它们存在的话。

它通过为任何请求者制造密钥，在开放网络上的主体之间提供相互认证和安全通信。还提供了通过网络安全传播这些密钥的机制。Kerberos不提供授权或记帐。但是，希望使用其密钥以安全地执行这些功能的应用程序。

定义

- **身份验证** — 确保您是自己所说的人，并且我们知道您是谁。
- **Client** — 可获取票证的实体。此实体通常是用户或主机。
- **凭据** — 与票证相同。
- **Daemon** — 为网络请求提供身份验证服务的程序，通常在UNIX主机上运行。
- **主机** — 可通过网络访问的计算机。
- **实例** - Kerberos主体的第二部分。它提供符合主设备资格的信息。实例可以为null。对于用户，通常使用实例来描述相应凭证的预期用途。对于主机，实例是完全限定的主机名。
- **Kerberos** — 在希腊神话中，三头狗守卫着冥界的入口。在计算机世界中，Kerberos是MIT开发的网络安全软件包。
- **KDC** — 密钥分发中心。发出Kerberos票证的计算机。
- **Keytab** — 包含一个或多个键的键表文件。主机或服务使用keytab文件的方式与用户使用其密码的方式大致相同。
- **NAS** — 网络接入服务器（Cisco机箱）或其他发出TACACS+身份验证和授权请求或发送记帐数据包的设备。
- **承担者** — 为可向其分配一组凭据的特定实体命名的字符串。它通常有三个部分，分别名为Primary、Instance和REALM。典型Kerberos主体的典型格式是**primary/instanceREALM**。
- **Primary** - Kerberos主体的第一部分。对于用户，它是用户名。对于服务，它是服务的名称。
- **REALM** — 由单个Kerberos数据库和一组密钥分发中心提供服务的逻辑网络。按照惯例，领域名称通常都是大写字母，以区分领域与Internet域。
- **服务** — 通过网络访问的任何程序或计算机。服务示例包括："host" — 主机（例如，当您使用Telnet和rsh时）"ftp" - FTP"krbtgt" — 身份验证；例如票证授予票证“pop” — 电子邮件
- **票证** — 用于验证特定服务的客户端身份的临时电子凭证集。
- **TGT** — 票证授予票证。一种特殊的Kerberos票证，允许客户端在同一Kerberos领域内获取其他Kerberos票证。给票票的一个很好的类比是3天的滑雪通行证，适用于4个不同的度假胜地。您在您决定去的任何度假胜地（直到过期）显示通行证，并收到该度假胜地的机票。一旦你拿到了电梯票，你就可以在度假地滑雪。如果第二天去另一个度假地，你再次出示通行证，你还会得到新度假地的额外机票。区别在于，Kerberos V5程序会注意到您有周末滑雪通行证，并为您

获取电梯票，因此您不必自己执行事务。

戈察

本节列出了您需要了解的几项：

- 确保删除配置文件中的所有尾随空格。尾随空格可能导致krb5kdc服务器出现问题。否则，您会收到一条消息，说“krb5kdc无法启动该领域的数据库。”
- 确保路由器上的时钟设置为与运行KDC服务器的UNIX主机相同的时间。为防止入侵者重置其系统时钟以继续使用过期票证，Kerberos V5设置为拒绝来自任何主机的票证请求，其时钟不在KDC的指定最大时钟偏差（如kdc.conf文件中指定）。 同样，主机配置为拒绝来自任何KDC的响应，其时钟不在主机的指定最大时钟偏差（如krb5.conf文件中指定）内。 最大时钟偏差的默认值为300秒（5分钟）。
- 确保DNS工作正常。Kerberos的几个方面依赖于名称服务。为了使Kerberos提供高级别的安全性，它比网络的其他部分对名称服务问题更敏感。您的域名系统(DNS)条目和主机必须具有正确的信息。主机名的每个规范必须是完全限定的主机名（包括域），并且主机的每个IP地址必须反向解析为规范名。
- Cisco IOS Kerberos V5支持不允许使用小写领域名，如果领域为小写，Cisco IOS中的Kerberos代码不会对用户进行身份验证。这已在思科IOS软件版本11.2(7)中修复。请参阅Cisco Bug ID CSCdj10598(仅限注册客户)。唯一的解决方法是使用大写的REALM名称（这是常规方法）。小写领域用于检索TGT，但不检索服务凭证。由于思科使用其新的TGT来在日志记录身份验证期间检索服务凭证（用于防止KDC欺骗攻击），因此使用小写领域的Kerberos身份验证始终会失败。
- 用于PPP PAP和CHAP的Kerberos V5可能会使路由器崩溃。这已在Cisco IOS软件版本11.2(6)中修复。请参阅Cisco Bug ID CSCdj08828(仅限注册的客户)。对此的解决方法是，通过异步模式interactive强制执行登录路由器，**而不在登录期间自动选择，然后**让用户手动启动PPP:
  ```
  aaa authentication ppp default if-needed krb5 local
  ```
- Kerberos V5不进行授权或记帐。你需要一些其他代码才能做到。

Cisco IOS路由器配置

本节中的配置描述了执行Kerberos V5的完全配置的AS5200路由器。此配置中的路由器使用Kerberos服务器对VTY会话和拨入以执行PPP和PAP身份验证的用户进行身份验证。

AS5200配置Kerberos V5

```
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

确保已为inetd设置正确的**端口**。

注意： 本示例使用包装。如果要加密的Telnet，则需要用字符化Telnet替换普通的Telnet，因此这些文件的外观不同。

为inetd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

接下来，您需要设置KDC服务器读取的几个Kerberos配置文件。有关这些参数含义的详细信息，请参阅《Kerberos安装指南》或《系统管理指南》。

```
# 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
     }
```

为KDC服务器设置数据库

接下来，您需要创建KDC服务器使用的数据库。

1. 输入命令**kdb5_util**:

```
# 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:
```

要通过TFTP使用kerberos srvtab remote命令从路由器**检索**srvtab口令，需**要执行此**操作。

```
# kadmin/dbutil/kdb5_util  stash -r CISCO.EDU
Enter KDC database master key:
```

2. 要将主体和用户添加到数据库，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. 获取当前数据库的列表：

```
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. 提取Cisco路由器表中的密钥：

```
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. 再看一下数据库：

```
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. 将keytab文件移动到路由器能够到达的位置：

```
# cp /etc/krb5.keytab /ts/
# chmod 777 /ts/krb5.keytab
```

9. 启动KDC服务器：

```
# kdc/krb5kdc
#
```

10. 检查以确保其实际运行：

```
# ps -A | grep  'krb5'
 6043 ??       I        0:00.01 kdc/krb5kdc
23427 ttypf    S  +     0:00.05 grep krb5
```

11. 强制路由器读取其密钥表条目：

```
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，确保一切就绪：

```
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. 打开调试并尝试登录路由器：

```
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

这是成功进行身份验证的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

本节包含各种潜在问题的场景。这些调试可帮助您快速发现问题。

领域名称错误

```
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不起作用

```
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
                                        ~~~~
```

路由器时钟不正确

```
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
----------------------
```

以下是用户看到的内容：

```
$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:
```

客户端不在Kerberos数据库中

```
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
```

客户端在数据库中，但使用了错误的密码

```
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
```

用户看到以下输出：

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

```
User Access Verification

Username: cisco1
Password:
% Access denied

Username:
```

路由器上的SRVTAB条目不正确

```
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
```

以下是用户看到的内容：

```
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*系统管理员指南*（包含标记的g-zipped文件）
2. 《Kerberos V5*安装指南*》
3. Kerberos V5 *UNIX用户指南*
4. Kerberos:网络身份验证协议
5. Kerberos网络身份验证服务（USC/ISI的GOST组）
6. 詹妮弗G斯坦纳，克利福德·诺伊曼，杰弗里·席勒。“Kerberos:An Authentication Service for Open Network Systems”，USENIX 1988年3月
7. S. P. Miller， B. C. Neuman， J. I. Schiller和J. H. Saltzer， "Kerberos Authentication and Authorization System，",12/21/87
8. R. M. Needham和M. D. Schroeder，《在大型计算机网络中使用加密进行身份验证》，ACM通讯，第21(12)卷，第993-999页（1978年12月）
9. V. L. Voydock和S. T. Kent，《高级网络协议中的安全机制》计算调查，第15(2)卷，ACM（1983年6月）
10. 李功，《A Security Risk of Diveng on Synchronized Clocks》，操作*系统评*论，第26卷，#1，第49-53页
11. C. Neuman和J. Kohl，“The Kerberos Network Authentication Service(V5)”，RFC 1510,1993年9月
12. B. Clifford Neuman和Theodore Ts'o，“Kerberos:An Authentication Service for Computer Networks，"IEEE Communications，32(9),1994年9月**注意**：其中许多文档(包括Neuman、Schiller和Steiner(#9)的文档)也可通过FTP从MIT Athena System — Kerberos Documentation获得。要获取RFC的副本，请参阅获取RFC和标准文档。

相关信息

- Kerberos 支持页
- 技术支持 - Cisco Systems