疑難排解和設定Kerberos V5使用者端支援

目錄

簡介

本文提供範例組態，以及常見問題的一些解決方案。本文還提供幫助您解決任何問題的技術。本文不解決核心化Telnet支援的問題。

本文中的多數內容來自隨Kerberos一起提供的免費文檔以及軟體包中各種可用的常見問題(FAQ)。配置來自功能正常的路由器和Kerberos KDC伺服器。

本文檔假定您已正確編譯並安裝了來自MIT的Kerberos軟體包的第5版當前版本。有關如何獲取、編譯和安裝Kerberos V5的資訊，請參閱本文結尾的參考。

另請注意，Kerberos V5支援需要Cisco IOS®軟體版本11.2或更高版本。這提供了對Kerberos V客戶端身份驗證的完全支援，包括憑據轉發。具有Kerberos V基礎架構的系統可以使用其金鑰發行中心(KDC)對終端使用者進行網路或路由器訪問身份驗證。這是一個客戶端實現，而不是Kerberos KDC實現。

Kerberos被認為是一種傳統的安全服務，在已使用Kerberos的網路中最為有用。

請參閱Cisco IOS軟體版本11.2發行說明，瞭解有關哪些版本包含此支援的詳細資訊。

有關後續Cisco IOS軟體版本中的Kerberos支援，請參閱Software Advisor(僅限註冊客戶)。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS軟體版本11.2及更新版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

Kerberos簡介

Kerberos是一種在物理上不安全的網路上使用的網路身份驗證協定。Kerberos基於Needham和Schroeder提出的金鑰分發模型。(請參閱本文檔的參考部分中的數字9。)它旨在通過使用金鑰加密為客戶端/伺服器應用程式提供強身份驗證。它允許通過網路通訊的實體互相證明其身份，同時防止竊聽或重放攻擊。它還提供了資料流完整性（如檢測修改）和保密性（如防止未經授權的讀取），其幫助是諸如DES的密碼系統。

Internet中使用的許多協定不提供任何安全性。用於「嗅探」網路密碼的工具通常由系統破解程式使用。因此，通過網路傳送未加密的密碼的應用程式易受攻擊。此外，其他客戶端/伺服器應用程式依賴客戶端程式對使用該程式的使用者的身份「誠實」。其他應用程式依賴客戶端將其活動限製為允許其進行的活動，伺服器不會執行其他強制措施。

有些站點試圖使用防火牆來解決其網路安全問題。防火牆假設「壞人」在外部，這通常是一種無效假設。然而，大多數造成更大破壞的電腦犯罪事件是由內部人員實施的。防火牆也有很大的缺點，因為它們限制了使用者使用網際網路的方式。

Kerberos是由MIT建立的，用於解決這些網路安全問題。Kerberos協定使用強加密技術，因此客戶端可以通過不安全的網路連線向伺服器證明其身份（反之亦然）。在客戶端和伺服器使用Kerberos來證明其身份之後，它們還可以對所有的通訊進行加密，以確保在業務過程中隱私和資料完整性。

Kerberos可以從MIT免費獲得，其版權許可通知與BSD操作和X11 Windowing系統使用的許可通知相似。MIT以源形式提供Kerberos。這樣做是為了讓任何希望使用該代碼的人可以親自檢視代碼，並向自己保證代碼是可信的。此外，對於那些希望依賴於專業支援的產品的人來說，Kerberos可

作為來自許多不同供應商的產品提供。

Kerberos V5客戶端支援基於MIT開發的Kerberos身份驗證系統。在Kerberos下，客戶端（通常是使用者或服務）將票證請求傳送到金鑰分發中心(KDC)。 KDC為客戶端建立票證授予票證(TGT)，使用客戶端的密碼作為金鑰對其進行加密，並將加密後的TGT傳送回客戶端。然後使用者端會嘗試使用密碼來解密TGT。如果使用者端成功解密TGT（例如使用者端提供正確密碼），則保留已解密的TGT。這表示客戶端身份的證明。

TGT會在指定的時間到期，它允許客戶端獲取其他票證，從而授予特定服務的許可權。這些附加票證的請求和授權是使用者透明的。

由於Kerberos會協商經過身份驗證、選擇性地加密，並在Internet上的任意兩點之間進行通訊，因此它提供的安全層不取決於客戶端所在的防火牆哪一端。Kerberos主要用於應用層協定（ISO第7級模型），例如Telnet或FTP，以提供使用者到主機的安全性。它也被用作資料流的隱式驗證系統(例如**SOCK_STREAM**)或RPC機制（ISO模型級別6），儘管使用頻率較低。 它也可以在較低級別用於主機到主機安全，例如IP、UDP或TCP（ISO第3級和第4級）等協定。 儘管這樣的實施非常罕見，即使它們真的存在。

它通過為任何請求者製造金鑰，在開放網路上的主體之間提供相互認證和安全通訊。還提供了一種用於使這些金鑰安全地通過網路傳播的機制。Kerberos不提供授權或記帳。但是，希望能夠使用其金鑰安全地執行這些功能的應用程式。

定義

- **驗**證 — 確保您就是您所說的人，並且我們瞭解您的身份。
- **客戶端** — 可以獲取票證的實體。此實體通常是使用者或主機。
- **憑**據 — 與票證相同。
- **守護程**序 — 通常運行在UNIX主機上的程式，為網路身份驗證請求提供服務。
- **主機** — 可以通過網路訪問的電腦。
- **例項**- Kerberos主體的第二部分。它提供限定主節點的資訊。例項可以為null。對於使用者，通常使用例項來描述相應憑證的預期用途。對於主機，例項是完全限定主機名。
- **Kerberos** — 在希臘神話中，守衛著進入冥界的三頭狗。在電腦領域，Kerberos是在MIT開發的一個網路安全包。
- **KDC** — 金鑰分發中心。發出Kerberos票證的電腦。
- **Keytab** — 包含一個或多個鍵的鍵表檔案。主機或服務使用keytab檔案的方式與使用者使用密碼的方式非常相似。
- **NAS** — 網路存取伺服器（思科方塊）或其他任何發出TACACS+驗證和授權要求，或傳送記帳封包的工具。
- **Principal** — 一個字串，它命名可向其分配一組憑據的特定實體。它通常有三個部分，分別名為Primary、Instance和REALM。典型Kerberos主體的典型格式為**primary/instanceREALM**。
- **Primary** - Kerberos主體的第一部分。使用者為使用者名稱。如果是服務，則為服務的名稱。
- **REALM** — 由單個Kerberos資料庫和一組金鑰分發中心服務的邏輯網路。按照慣例，領域名稱通常都是大寫字母，以區分領域與Internet域。
- **Service** — 通過網路訪問的任何程式或電腦。服務示例包括："host" — 主機（例如，使用Telnet和rsh時）"ftp" - FTP"krbtgt" — 身份驗證；例如票證授予票證"pop" — 電子郵件
- **票證** — 用於驗證特定服務的客戶端身份的臨時電子憑據集。
- **TGT** — 票證授予票證。一個特殊的Kerberos票證，允許客戶端獲取同一Kerberos領域內的其他Kerberos票證。與這張門票相似的是，一張三天的滑雪通行證，在四個不同的度假勝地很合適。在決定去的任何一個度假勝地展示該通行證（直到它到期），然後你將收到該度假勝地的電梯票。一旦你買了電梯票，你就可以想在那個度假村滑雪了。如果你第二天去另一個度假村

，又會展示你的通行證，你就能得到一張新度假村的額外電梯票。不同之處在於，Kerberos V5程式會注意到您有週末滑雪通行證，並且會收到電梯票，因此您不必親自執行交易。

懂了

本節列出了需要注意的幾個事項：

- 確保刪除配置檔案中的所有尾隨空格。尾隨空格可導致krb5kdc伺服器出現問題。否則，您會收到一條消息「krb5kdc cannot start the database for the realm」。
- 確保將路由器上的時鐘設定為與運行KDC伺服器的UNIX主機相同的時間。為了防止入侵者重置其系統時鐘以繼續使用過期的票證，Kerberos V5被設定為拒絕來自任何主機的票證請求，這些主機的時鐘不在KDC指定的最大時鐘偏差內（如kdc.conf檔案中指定的）。 同樣，主機配置為拒絕來自任何時鐘不在主機指定的最大時鐘偏差範圍之內的KDC的響應（如krb5.conf檔案中指定的）。 最大時鐘偏差的預設值為300秒（五分鐘）。
- 確保DNS工作正常。Kerberos的幾個方面依賴於名稱服務。為了讓Kerberos提供高級別的安全性，它對名稱服務問題的敏感度要高於網路的其他部分。請務必確保您的域名系統(DNS)條目和主機具有正確的資訊。主機名的每個規範名稱必須是完全限定主機名（包括域），主機的每個IP地址都必須反向解析為規範名稱。
- Cisco IOS Kerberos V5支援不允許使用小寫領域名稱，如果領域為小寫，Cisco IOS中的Kerberos代碼不會驗證使用者。已在Cisco IOS軟體版本11.2(7)中修正。請參閱Cisco錯誤ID CSCdj10598(僅限註冊客戶)。唯一的解決方法是使用大寫領域名稱（這是常規方法）。小寫領域用於檢索TGT，而不是服務憑據。由於Cisco在日誌驗證過程中使用新的TGT來檢索服務憑據（用於防止KDC欺騙攻擊），因此使用小寫領域的Kerberos身份驗證始終會失敗。
- 適用於PPP PAP和CHAP的Kerberos V5可能會使路由器崩潰。已在Cisco IOS軟體版本11.2(6)中修正。請參閱Cisco錯誤ID CSCdj08828 (僅限註冊客戶)。此問題的解決方法是通過**非同步模式互動**強制執行exec登入到路由器，而不在登入期間自動選擇，然後讓使用者手動啟動PPP:
  ```
  aaa authentication ppp default if-needed krb5 local
  ```
- Kerberos V5不執行授權或記帳。您需要一些其它代碼才能執行此操作。

Cisco IOS路由器配置

本節中的組態說明執行Kerberos V5的完整設定AS5200路由器。此組態中的路由器使用Kerberos伺服器來驗證VTY作業階段和撥入以使用PAP驗證執行PPP的使用者。

採用Kerberos V5的AS5200組態

```
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

確保為inetd設定了正確的**埠**。

附註： 此示例使用包裝器。如果要加密的Telnet，則需要使用核心化的Telnet替換普通的Telnet，因此這些檔案的外觀會有所不同。

為inetd設定埠

```
# 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
-----------------------------------------------------------------
```

設定Kerberos配置檔案

接下來，需要設定一些KDC伺服器讀取的Kerberos配置檔案。有關這些引數含義的詳細資訊，請參閱Kerberos安裝指南或系統管理員指南 。

```
# 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
     }
```

為KDC伺服器設定資料庫

接下來，需要建立KDC伺服器使用的資料庫。

1. 輸入命令**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:
```

要使用**kerberos srvtab remote**命令通過TFTP從路由器檢索**srvtab**口令，需要使用此命令。

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

2. 若要將承擔者和使用者新增到資料庫，請使用**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. 新增使用者：

```
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. 獲取當前資料庫的清單：

```
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. 為思科路由器新增專案：

```
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. 為Cisco路由器提取表項：

```
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. 再看一下資料庫：

```
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. 將keytab檔案移動到路由器能夠到達的位置：

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

9. 啟動KDC伺服器：

```
# kdc/krb5kdc
#
```

10. 檢查以確保它實際運行：

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

11. 強制路由器讀取其金鑰表條目：

```
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. 檢查路由器以確保一切就緒：

```
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. 開啟偵錯並嘗試登入路由器：

```
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
```

調試輸出示例

以下是成功進行身份驗證的PPP使用者。

```
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
```

疑難排解

本節包含針對潛在問題的各種方案。這些調試可幫助您快速發現問題。

錯誤的領域名稱

```
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
                                          ~~~~
```

路由器時鐘不正確

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

以下是使用者看到的內容：

```
$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:
```

客戶端不在Kerberos資料庫中

```
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
```

客戶端在資料庫中，但使用了錯誤的密碼

```
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
```

使用者看到以下輸出：

```
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條目不正確

```
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
```

以下是使用者看到的內容：

```
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:
```

參考資料

1. Kerberos V5系*統管理員指南*（位於帶跟蹤的g壓縮檔案中）
2. Kerberos V5安*裝指南*
3. 《Kerberos V5 *UNIX使用手冊*》
4. Kerberos:網路身份驗證協定
5. Kerberos網路驗證服務（USC/ISI的GOST群組）
6. 詹妮弗G斯坦納，克利福德·紐曼，傑弗里I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驗證和授權系統」，12/21/87
8. R. M. Needham和M. D. Schroeder，「Using Encryption for Authentication in Large Networks of Computers」，《ACM通訊》，第21(12)卷，第993-999頁（1978年12月）
9. V. L. Voydock和S. T. Kent，「Security Mechanism in High-Level Network Protocols」，《*Computing Survey*》，第15(2)卷，ACM（1983年6月）
10. 李貢，「依賴於同步時鐘的安全風險」，《作業系統*回顧*》，第26卷，#1頁，第49-53頁
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（電腦網路認證服務）」，IEEE Communications，32(9),1994年9月**注意：**其中的許多文檔，包括Neuman、Schiller和Steiner(#9)的文檔，也可通過FTP從MIT Athena System — Kerberos Documentation獲得。要獲取RFC的副本，請參閱獲取RFC和標準文檔。

相關資訊

- **Kerberos支援頁面**
- **技術支援 - Cisco Systems**