Risoluzione dei problemi e configurazione del supporto client Kerberos V5

Sommario

Introduzione

Questo documento offre un esempio di configurazione e alcune soluzioni a problemi comuni. In questo documento vengono inoltre illustrate le tecniche per la risoluzione dei problemi. Questo documento non risolve il supporto Telnet kerberizzato.

La maggior parte di questo materiale proviene dalla documentazione disponibile gratuitamente con Kerberos e da varie domande frequenti (FAQ) disponibili sul pacchetto. Le configurazioni provengono da un router funzionale e da un server KDC Kerberos.

In questo documento si presume che sia stata compilata e installata correttamente una versione corrente della versione 5 del pacchetto Kerberos dal MIT. Fare riferimento ai riferimenti alla fine di questo articolo per informazioni su come ottenere, compilare e installare Kerberos V5.

Notare anche che il software Cisco IOS® versione 11.2 o successive è richiesto per il supporto di Kerberos V5. In questo modo viene fornito il supporto completo dell'autenticazione del client Kerberos V, che include l'inoltro delle credenziali. I sistemi con infrastruttura Kerberos V possono utilizzare i KDC (Key Distribution Center) per autenticare gli utenti finali per l'accesso alla rete o al router. Si tratta di un'implementazione client e non di un'implementazione KDC Kerberos.

Kerberos è considerato un servizio di sicurezza legacy ed è utile soprattutto nelle reti che utilizzano già Kerberos.

Per informazioni più dettagliate sulle versioni che includono questo supporto, consultare le note sulla versione 11.2 del software Cisco IOS.

Per il supporto di Kerberos nelle versioni software Cisco IOS successive, fare riferimento al Software Advisor (solo utenti registrati).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS release 11.2 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Introduzione a Kerberos

Kerberos è un protocollo di autenticazione di rete da utilizzare su reti fisicamente non sicure. Kerberos si basa sul modello di distribuzione chiave presentato da Needham e Schroeder. Vedere il Numero 9 nella sezione Riferimenti di questo documento. È progettato per fornire un'autenticazione efficace per le applicazioni client/server tramite la crittografia a chiave segreta. Consente alle entità che comunicano in rete di dimostrare la propria identità l'una con l'altra, impedendo attacchi di tipo intercettazione o ripetizione. Fornisce inoltre l'integrità del flusso di dati (ad esempio il rilevamento di modifiche) e la segretezza (ad esempio la prevenzione della lettura non autorizzata) con l'aiuto di sistemi di crittografia come DES.

Molti dei protocolli utilizzati in Internet non garantiscono alcuna protezione. Gli strumenti utilizzati

per "sniffare" le password al di fuori della rete sono comunemente utilizzati dai cracker di sistema. Di conseguenza, le applicazioni che inviano una password sulla rete senza crittografia sono vulnerabili. Inoltre, altre applicazioni client/server si affidano al programma client per essere "onesti" sull'identità dell'utente che lo utilizza. Altre applicazioni si affidano al client per limitare le proprie attività a quelle consentite, senza alcuna altra imposizione da parte del server.

Alcuni siti tentano di utilizzare i firewall per risolvere i problemi di protezione della rete. I firewall presumono che "i cattivi" siano all'esterno, il che è spesso un presupposto non valido. Tuttavia, la maggior parte degli incidenti legati al crimine informatico che causano maggiori danni sono stati commessi da addetti ai lavori. I firewall hanno inoltre un notevole svantaggio in quanto limitano le modalità di utilizzo di Internet da parte degli utenti.

Kerberos è stato creato dal MIT come soluzione a questi problemi di sicurezza della rete. Il protocollo Kerberos utilizza la crittografia avanzata, in modo che un client possa dimostrare la propria identità a un server (e viceversa) attraverso una connessione di rete non protetta. Dopo che un cliente e un server hanno utilizzato Kerberos per dimostrare la propria identità, possono anche crittografare tutte le loro comunicazioni per garantire la privacy e l'integrità dei dati mentre svolgono la loro attività.

Kerberos è liberamente disponibile dal MIT, con un avviso di autorizzazione di copyright simile a quello utilizzato per il sistema operativo BSD e X11 Windowing. MIT fornisce Kerberos in forma di origine. In questo modo, chiunque desideri utilizzarlo può controllare il codice e assicurarsi che sia attendibile. Inoltre, per coloro che preferiscono affidarsi a un prodotto supportato da un professionista, Kerberos è disponibile come prodotto di diversi fornitori.

Il supporto client Kerberos V5 è basato sul sistema di autenticazione Kerberos sviluppato presso il MIT. In Kerberos, un client (in genere un utente o un servizio) invia una richiesta di ticket al Centro distribuzione chiavi (KDC). Il KDC crea un ticket di concessione ticket (TGT) per il client, lo cripta con l'aiuto della password del client come chiave e invia il TGT crittografato al client. Il client tenta quindi di decrittografare il TGT, con l'aiuto della relativa password. Se il client decrittografa correttamente il TGT (ad esempio, se fornisce la password corretta), mantiene il TGT decrittografato. Indica la prova dell'identità del client.

Il TGT, che scade a un orario specificato, consente al cliente di ottenere ulteriori ticket, che danno l'autorizzazione per servizi specifici. Le richieste e le concessioni di questi biglietti aggiuntivi sono trasparenti per l'utente.

Poiché Kerberos esegue la negoziazione con l'autenticazione, è facoltativamente crittografato e comunica tra due punti qualsiasi su Internet, fornisce un livello di protezione che non dipende dal lato di un firewall in cui si trova il client. Kerberos è utilizzato principalmente nei protocolli a livello di applicazione (modello ISO livello 7), ad esempio Telnet o FTP, per garantire la protezione da host a utente. Viene anche utilizzato, sebbene meno frequentemente, come sistema di autenticazione implicita del flusso di dati (come SOCK_STREAM) o meccanismi RPC (modello ISO livello 6). Può inoltre essere utilizzato a un livello inferiore per la sicurezza host-host, in protocolli quali IP, UDP o TCP (modelli ISO livelli 3 e 4). Anche se, tali implementazioni sono rare, se esistono affatto.

Prevede l'autenticazione reciproca e la comunicazione sicura tra gli utenti/gruppi/ruoli su una rete aperta mediante la produzione di chiavi segrete per qualsiasi utente. Viene inoltre fornito un meccanismo per la propagazione sicura di queste chiavi segrete attraverso la rete. Kerberos non prevede l'autorizzazione o la contabilità. Tuttavia, le applicazioni che desiderano utilizzare le proprie chiavi segrete per eseguire tali funzioni in modo sicuro.

Definizioni

- **Autenticazione**: verificare che l'utente sia quello che si dice di essere e che l'utente sia noto.
- **Client** - Entità che può ottenere un ticket. Questa entità è in genere un utente o un host.
- **Credenziali** - Equivalente ai ticket.
- **Daemon**: programma, in genere eseguito su un host UNIX, che gestisce le richieste di autenticazione della rete.
- **Host** - Computer a cui è possibile accedere in rete.
- **Istanza** - Seconda parte di un'entità Kerberos. Fornisce informazioni che qualificano il sito principale. L'istanza può essere null. Nel caso di un utente, l'istanza viene spesso utilizzata per descrivere l'utilizzo previsto delle credenziali corrispondenti. Nel caso di un host, l'istanza è il nome host completo.
- **Kerberos** - Nella mitologia greca, il cane a tre teste che sorveglia l'ingresso dell'oltretomba. Nel mondo dei computer, Kerberos è un pacchetto di sicurezza di rete sviluppato al MIT.
- **KDC**: centro distribuzione chiavi. Una macchina che emette biglietti Kerberos.
- **Tab** - File di tabella dei tasti contenente uno o più tasti. Un host o un servizio utilizza un file keytab nello stesso modo in cui un utente utilizza la propria password.
- **NAS**: un server di accesso alla rete (una confezione di Cisco) o qualsiasi altra soluzione che richiede l'autenticazione e l'autorizzazione TACACS+ o che invia pacchetti di accounting.
- **Principal** - Stringa che denomina un'entità specifica alla quale è possibile assegnare un set di credenziali. In genere sono presenti tre parti denominate Primario, Istanza e REALM.Il formato tipico di un principal Kerberos tipico è **primary/instanceREALM**.
- **Principale** (**Primary**) - Prima parte di un principal Kerberos. Nel caso di un utente, è il nome utente. Nel caso di un servizio, è il nome del servizio.
- **REALM**: la rete logica servita da un singolo database Kerberos e da un insieme di centri di distribuzione delle chiavi. Per convenzione, i nomi dei realm sono generalmente lettere maiuscole, per differenziare il realm dal dominio Internet.
- **Servizio (Service**) - Qualsiasi programma o computer a cui si accede in rete. Alcuni esempi di servizi:"host": un host, ad esempio quando si utilizzano Telnet e rsh"ftp"—FTP"krbtgt"—autenticazione; come il ticket di concessione"pop"—E-mail
- **Ticket**: insieme temporaneo di credenziali elettroniche che verificano l'identità di un client per un particolare servizio.
- **TGT** - Ticket-Granting Ticket. Uno speciale ticket Kerberos che consente al cliente di ottenere ulteriori ticket Kerberos all'interno dello stesso realm Kerberos.Una buona analogia per il biglietto è uno skipass di tre giorni valido in quattro diversi resort. Mostrare il pass in qualsiasi località si decide di andare (fino alla scadenza), e si riceve un biglietto di ascensore per quella località. Una volta che hai il biglietto per l'ascensore, puoi sciare tutto ciò che vuoi in quella località. Se andate in un altro resort il giorno successivo, mostrate ancora una volta il vostro pass, e ottenete un biglietto di ascensore aggiuntivo per il nuovo resort. La differenza è che i programmi Kerberos V5 notano che hai lo skipass per il weekend e ottieni il biglietto per l'ascensore per te, così non devi eseguire le transazioni da solo.

Ottenuto

In questa sezione sono elencati diversi elementi che è necessario conoscere:

- Accertatevi di rimuovere tutti gli spazi finali nei file di configurazione. Gli spazi finali possono

causare problemi con il server krb5kdc. In caso contrario, viene visualizzato il messaggio "krb5kdc non è in grado di avviare il database per il realm."

- Verificare che l'orologio sul router sia impostato sulla stessa ora dell'host UNIX che esegue il server KDC. Per impedire agli intrusi di reimpostare gli orologi di sistema per continuare a utilizzare i ticket scaduti, Kerberos V5 è configurato per rifiutare le richieste di ticket da qualsiasi host il cui orologio non rientra nello sfasamento massimo di clock specificato del KDC (come specificato nel file kdc.conf). Analogamente, gli host sono configurati in modo da rifiutare le risposte da qualsiasi KDC il cui clock non rientri nello sfasamento massimo di clock specificato per l'host (come specificato nel file krb5.conf). Il valore predefinito per l'inclinazione massima dell'orologio è 300 secondi (cinque minuti).
- Assicurarsi che il DNS funzioni correttamente. Diversi aspetti di Kerberos si basano sul servizio di denominazione. Per garantire un livello elevato di protezione, Kerberos è più sensibile ai problemi relativi al servizio nomi rispetto ad altre parti della rete. È importante che le voci DNS (Domain Name System) e gli host dispongano delle informazioni corrette. Ogni canonico del nome host deve essere il nome host completo (che include il dominio) e ogni indirizzo IP dell'host deve essere risolto in modo inverso nel nome canonico.
- Il supporto di Cisco IOS Kerberos V5 non consente l'utilizzo di nomi di area di autenticazione in minuscolo e il codice Kerberos in Cisco IOS non autentica gli utenti se l'area di autenticazione è in minuscolo. Questa condizione è stata risolta nel software Cisco IOS versione 11.2(7).Fare riferimento all'ID bug Cisco CSCdj10598 (solo utenti registrati).L'unica soluzione è utilizzare i nomi dei realm in lettere maiuscole (il tradizionale).I realm minuscoli funzionano per recuperare un TGT, ma non una credenziale del servizio. Poiché Cisco utilizza il nuovo TGT per recuperare le credenziali di un servizio (utilizzate per impedire l'attacco di spoofing KDC) durante l'autenticazione di registrazione, l'autenticazione Kerberos che utilizza realm minuscoli ha sempre esito negativo.
- Kerberos V5 per PPP PAP e CHAP può bloccare il router. Questa condizione è stata risolta nel software Cisco IOS versione 11.2(6).Fare riferimento all'ID bug Cisco CSCdj08828 (solo utenti registrati).Per risolvere questo problema, forzare l'accesso exec al router in **modalità asincrona interattiva** senza **selezione automatica durante l'accesso automatico** e fare in modo che l'utente avvii manualmente il protocollo PPP:
  ```
  aaa authentication ppp default if-needed krb5 local
  ```
- Kerberos V5 non esegue l'autorizzazione o l'accounting. A tale scopo, è necessario immettere altro codice.

Configurazione router Cisco IOS

Nella configurazione di questa sezione è illustrato un router AS5200 completamente configurato con Kerberos V5. Il router in questa configurazione utilizza il server Kerberos per autenticare sia le sessioni VTY sia gli utenti che effettuano la connessione per eseguire il protocollo PPP con l'autenticazione PAP.

Configurazione AS5200 con 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
```

Configurazione KDC Kerberos

Accertarsi di disporre delle porte corrette per **inetd**.

Nota: In questo esempio vengono utilizzati i wrapper. Se si desidera un Telnet crittografato, è necessario sostituire il Telnet normale con il Telnet kerberizzato, in modo che questi file abbiano un aspetto diverso.

Configura porte per inetd

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

Configurazione dei file di configurazione di Kerberos

Èquindi necessario configurare alcuni file di configurazione Kerberos letti dal server KDC. Per ulteriori informazioni sul significato di questi parametri, consultare la Guida all'installazione di Kerberos o il manuale System Admin Guide .

```
# 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
     }
```

Imposta il database per il server KDC

Èquindi necessario creare il database utilizzato dal server KDC.

1. Immettere il comando **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:
```

Questa operazione è necessaria per recuperare la password **srvtab** dal router tramite il protocollo TFTP con il comando **remoto kerberos srvtab**.

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

2. Per aggiungere entità e utenti al database, utilizzare il comando **kadmin.local**:

```
# 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. Aggiungi utente:

```
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. Ottenere un elenco del database corrente:

```
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. Aggiungere la voce al router Cisco:

```
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. Estrarre una chiave nella tabella per il router Cisco:

```
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. Esaminare nuovamente il database:

```
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. Spostare il file keytab in un punto in cui il router sia in grado di accedervi:

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

9. Avviare il server KDC:

```
# kdc/krb5kdc
#
```

10. Verificare che venga eseguito:

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

11. Forzare il router a leggere la voce della tabella delle chiavi:

```
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. Controllare il router per assicurarsi che sia tutto pronto:

```
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. Attivare il debug e provare ad accedere al router:

```
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
```

Output di esempio del comando debug

Di seguito è riportato un utente PPP che esegue correttamente l'autenticazione.

```
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
```

Risoluzione dei problemi

In questa sezione sono disponibili diversi scenari per i potenziali problemi. Questi debug consentono di individuare rapidamente un problema.

Nome area autenticazione errato

```
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 non funziona

```
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
                                        ~~~~
```

Orologio del router non corretto

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

Di seguito sono riportati i contenuti visualizzati dall'utente:

```
$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:
```

Client non nel database Kerberos

```
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
```

Il client si trova nel database ma utilizza una password errata

```
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
```

L'utente visualizza questo output:

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


User Access Verification

Username: cisco1
Password:
% Access denied

Username:
```

Voce SRVTAB non corretta sul router

```
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
```

Di seguito sono riportati i contenuti visualizzati dall'utente:

```
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:
```

Riferimenti

1. *Guida dell'amministratore di sistema di* Kerberos V5 (disponibile in un file tarato, g-zipped)
2. *Guida all'installazione di* Kerberos V5
3. *Guida per l'utente di* Kerberos V5 *UNIX*
4. Kerberos: Protocollo di autenticazione di rete
5. Servizio di autenticazione di rete Kerberos (gruppo GOST di USC/ISI)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. "Kerberos: An Authentication Service for Open Network Systems ", USENIX marzo 1988
7. S. P. Miller, B. C. Neuman, J. I. Schiller, e J. H. Saltzer, "Kerberos Authentication and Authorization System,", 21/12/87
8. R. M. Needham e M. D. Schroeder, Using Encryption for Authentication in Large Networks of Computers, Comunicazioni dell'ACM, vol. 21(12), pp. 993-999 (dicembre 1978)
9. V. L. Voydock e S. T. Kent, "Security Mechanism in High-Level Network Protocols", *Computing Surveys*, vol. 15(2), ACM (giugno 1983)
10. Li Gong, "A Security Risk of Dependent on Synchronized Clock", *Operating Systems Review*, Vol 26, n. 1, pp 49-53
11. C. Neuman e J. Kohl, "The Kerberos Network Authentication Service (V5)," RFC 1510, settembre 1993
12. B. Clifford Neuman e Theodore Ts'o, "Kerberos: An Authentication Service for Computer Networks," Comunicazioni IEEE, 32(9), settembre 1994**Nota:** molti di questi documenti, tra cui quello di Neuman, Schiller e Steiner (n. 9) sono disponibili anche via FTP da MIT Athena System — Kerberos Documentation . Per ottenere copie delle RFC, consultare la sezione Recupero di RFC e documenti sugli standard.

Informazioni correlate

- Pagina di supporto Kerberos
- Supporto tecnico – Cisco Systems