Resolución de problemas y configuración del soporte del cliente Kerberos V5

Contenido

Introducción

Este documento proporciona un ejemplo de configuración, así como algunas soluciones a problemas comunes. En este documento también se proporcionan técnicas que le ayudarán a resolver cualquier problema. Este documento no aborda el soporte de Telnet con kerberized.

La mayor parte de este material en este artículo proviene de la documentación disponible libremente que viene con Kerberos y de varias preguntas frecuentes (FAQ) disponibles en el paquete. Las configuraciones procedían de un router funcional y del servidor Kerberos KDC.

Este documento asume que ha compilado e instalado correctamente una versión actual de la versión 5 del paquete Kerberos desde MIT. Consulte las referencias al final de este artículo para obtener información sobre cómo obtener, compilar e instalar Kerberos V5.

Tenga en cuenta también que Cisco IOS® Software Release 11.2 o posterior es necesario para el soporte Kerberos V5. Esto proporciona soporte completo para la autenticación del cliente Kerberos V, que incluye el reenvío de credenciales. Los sistemas que tienen infraestructuras Kerberos V pueden utilizar sus centros de distribución de claves (KDC) para autenticar a los usuarios finales para el acceso a la red o al router. Esta es una implementación de cliente y no una implementación de Kerberos KDC.

Kerberos se considera un servicio de seguridad heredado y es más beneficioso en redes que ya utilizan Kerberos.

Refiérase a las notas de la versión 11.2 del software Cisco IOS para obtener información más detallada sobre qué versiones incluyen este soporte.

Para obtener soporte de Kerberos en las versiones posteriores de Cisco IOS Software, refiérase a Software Advisor (sólo clientes registrados) .

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 11.2 y posteriores del software del IOS de Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Introducción a Kerberos

Kerberos es un protocolo de autenticación de red para su uso en redes físicamente inseguras. Kerberos se basa en el modelo de distribución de claves presentado por Needham y Schroeder. (Véase el número 9 en la sección Referencias de este documento. Se ha diseñado para proporcionar una autenticación sólida para las aplicaciones cliente/servidor mediante el uso de criptografía de clave secreta. Permite a las entidades que se comunican a través de redes probar su identidad entre sí, al tiempo que evita las intercepciones o los ataques de repetición. También se prevé la integridad del flujo de datos (como la detección de modificaciones) y el secreto (como la prevención de la lectura no autorizada) con la ayuda de sistemas criptográficos como DES.

Muchos de los protocolos utilizados en Internet no proporcionan ninguna seguridad. Las herramientas usadas para "detectar" contraseñas fuera de la red son de uso común por parte de

los sistemas crackers. Por lo tanto, las aplicaciones que envían una contraseña a través de la red sin cifrar son vulnerables. Además, otras aplicaciones cliente/servidor confían en el programa cliente para ser "honestas" sobre la identidad del usuario que la utiliza. Otras aplicaciones dependen del cliente para restringir sus actividades a las que está autorizado a realizar, sin ninguna otra aplicación por parte del servidor.

Algunos sitios intentan utilizar firewalls para resolver sus problemas de seguridad de red. Los firewalls asumen que "los malos" están fuera, lo que a menudo es una suposición inválida. Sin embargo, la mayoría de los incidentes de delitos informáticos que causan más daños han sido llevados a cabo por personas con información privilegiada. Los firewalls también presentan una desventaja significativa, ya que restringen el modo en que los usuarios pueden utilizar Internet.

El MIT creó Kerberos como solución a estos problemas de seguridad de la red. El protocolo Kerberos utiliza criptografía segura, de modo que un cliente puede probar su identidad a un servidor (y viceversa) a través de una conexión de red insegura. Después de que un cliente y un servidor hayan utilizado Kerberos para probar su identidad, también pueden cifrar todas sus comunicaciones para garantizar la privacidad y la integridad de los datos a medida que avanzan en su negocio.

Kerberos está disponible gratuitamente desde el MIT, bajo un aviso de permiso de autor que es similar al utilizado para el funcionamiento de BSD y el sistema de Windows X11. MIT proporciona Kerberos en forma de origen. Esto se hace para que cualquiera que desee usarlo pueda buscar el código por sí mismo y asegurarse de que el código es confiable. Además, para aquellos que prefieren confiar en un producto con soporte profesional, Kerberos está disponible como producto de muchos proveedores diferentes.

El soporte de cliente Kerberos V5 se basa en el sistema de autenticación Kerberos desarrollado en MIT. En Kerberos, un cliente (generalmente un usuario o un servicio) envía una solicitud de ticket al Centro de distribución de claves (KDC). La KDC crea un ticket de concesión de entradas (TGT) para el cliente, lo cifra con la ayuda de la contraseña del cliente como clave y envía la TGT cifrada de vuelta al cliente. El cliente entonces intenta descifrar la TGT, con la ayuda de su contraseña. Si el cliente descifra correctamente la TGT (por ejemplo, si el cliente da la contraseña correcta), mantiene la TGT descifrada. Esto indica la prueba de la identidad del cliente.

La TGT, que vence en un momento determinado, permite al cliente obtener entradas adicionales, que dan permiso para servicios específicos. Las solicitudes y subvenciones de estas entradas adicionales son transparentes para el usuario.

Dado que Kerberos negocia autenticado, está cifrado opcionalmente y se comunica entre dos puntos cualesquiera en Internet, proporciona una capa de seguridad que no depende de qué lado de un firewall se encuentre uno de los clientes. Kerberos se utiliza principalmente en los protocolos de nivel de aplicación (nivel 7 del modelo ISO), como Telnet o FTP, para proporcionar seguridad de usuario a host. También se utiliza, aunque con menor frecuencia, como el sistema de autenticación implícita de la secuencia de datos (como SOCK_STREAM) o mecanismos RPC (modelo ISO de nivel 6). También se puede utilizar en un nivel inferior para la seguridad de host a host, en protocolos como IP, UDP o TCP (niveles de modelo ISO 3 y 4). Aunque esas implementaciones son poco frecuentes, si es que existen.

Prevé la autenticación mutua y la comunicación segura entre los principales en una red abierta mediante la fabricación de claves secretas para cualquier solicitante. También se proporciona un mecanismo para que estas claves secretas se propaguen de forma segura a través de la red. Kerberos no prevé la autorización ni la contabilidad. Sin embargo, las aplicaciones que deseen utilizar sus claves secretas para realizar esas funciones de forma segura.

Definiciones

- **Autenticación**: asegúrese de ser quien dice ser y de saber quién es.
- **Cliente**: entidad que puede obtener un ticket. Esta entidad suele ser un usuario o un host.
- **Credenciales**: igual que las entradas.
- **Daemon**: un programa, normalmente uno que se ejecuta en un host UNIX, que atiende las solicitudes de autenticación de la red.
- **Host**: equipo al que se puede acceder a través de una red.
- **Instancia**: la segunda parte de una entidad principal Kerberos. Proporciona información que califica al primario. La instancia puede ser nula. En el caso de un usuario, la instancia se utiliza a menudo para describir el uso esperado de las credenciales correspondientes. En el caso de un host, la instancia es el nombre de host completo.
- **Kerberos**: En la mitología griega, el perro de tres cabezas que protege la entrada al submundo. En el mundo de los ordenadores, Kerberos es un paquete de seguridad de red desarrollado en MIT.
- **KDC**: Centro de distribución de claves. Una máquina que emite entradas Kerberos.
- **Pestaña**: archivo de tabla de claves que contiene una o más claves. Un host o servicio utiliza un archivo de ficha de clave de la misma manera que un usuario utiliza su contraseña.
- **NAS**: un servidor de acceso a la red (una caja de Cisco) o cualquier otra cosa que realice solicitudes de autenticación y autorización TACACS+, o que envíe paquetes de contabilidad.
- **Principal**: cadena que nombra una entidad específica a la que se puede asignar un conjunto de credenciales. Generalmente, tiene tres partes denominadas Primario, Instancia y REALM.El formato típico de un principal Kerberos típico es **primary/instanceREALM**.
- **Primario**: la primera parte de un principal Kerberos. En el caso de un usuario, es el nombre de usuario. En el caso de un servicio, es el nombre del servicio.
- **REALM**: la red lógica atendida por una única base de datos Kerberos y un conjunto de Centros de Distribución de Claves. Por convención, los nombres de dominio son generalmente letras mayúsculas, para diferenciar el rango del dominio de Internet.
- **Servicio**: cualquier programa o equipo al que se accede a través de una red. Algunos ejemplos de servicios son:"host": un host (por ejemplo, cuando utiliza Telnet y rsh)"ftp"—FTP"krbtgt": autenticación; tales como el billete que concede el billete"pop": correo electrónico
- **Venta**: conjunto temporal de credenciales electrónicas que verifican la identidad de un cliente para un servicio determinado.
- **TGT**: Billete que concede entradas. Un ticket Kerberos especial que permite al cliente obtener entradas Kerberos adicionales dentro del mismo rango Kerberos.Una buena analogía para el billete que concede el boleto es un pase de esquí de tres días que es bueno en cuatro complejos turísticos diferentes. Se muestra el pase a cualquier lugar al que se decida ir (hasta que caduque) y se le entrega un billete de ascensor para ese complejo. Una vez que tengas el ticket de ascensor, podrás esquiar todo lo que quieras en el complejo. Si vas a otro complejo al día siguiente, te volverás a mostrar el pase y te traen un billete de ascensor para el nuevo complejo. La diferencia es que los programas Kerberos V5 advierten que usted tiene el pase de esquí del fin de semana y obtiene el ticket de ascensor para usted, así que no tiene que realizar las transacciones usted mismo.

Gotcha

En esta sección se enumeran varios elementos que debe tener en cuenta:

- Asegúrese de quitar todos los espacios finales de los archivos de configuración. Los espacios de seguimiento pueden causar problemas con el servidor krb5kdc. De lo contrario, puede obtener un mensaje que diga "krb5kdc no puede iniciar la base de datos para el rango".
- Asegúrese de que el reloj del router esté configurado al mismo tiempo que el host UNIX que ejecuta el servidor KDC. Para evitar que los intrusos restablezcan sus relojes del sistema para seguir usando las notificaciones vencidas, Kerberos V5 se configura para rechazar las solicitudes de entradas de cualquier host cuyo reloj no esté dentro del valor máximo especificado del KDC (como se especifica en el archivo kdc.conf). De manera similar, los hosts se configuran para rechazar las respuestas de cualquier KDC cuyo reloj no esté dentro del intervalo máximo de reloj especificado del host (como se especifica en el archivo krb5.conf). El valor predeterminado para la desviación máxima del reloj es de 300 segundos (cinco minutos).
- Asegúrese de que DNS funciona correctamente. Varios aspectos de Kerberos dependen del servicio de nombres. Para que Kerberos proporcione su alto nivel de seguridad, es más sensible a los problemas de servicio de nombres que algunas otras partes de su red. Es importante que las entradas del sistema de nombres de dominio (DNS) y los hosts tengan la información correcta. Cada canónico del nombre de host debe ser el nombre de host completo (que incluya el dominio), y cada dirección IP del host debe resolver en sentido inverso el nombre canónico.
- El soporte de Kerberos V5 de Cisco IOS no permite el uso de nombres de rango en minúsculas y el código Kerberos en Cisco IOS no autentica a los usuarios si el rango está en minúsculas. Esto se corrigió en la versión 11.2(7) del software del IOS de Cisco.Consulte Cisco bug ID CSCdj10598 (sólo clientes registrados) .La única solución alternativa es utilizar nombres REALM en mayúscula (que es convencional).Los rangos en minúsculas funcionan para recuperar una TGT, pero no una credencial de servicio. Dado que Cisco utiliza su nueva TGT para recuperar una credencial de servicio (utilizada para evitar el ataque de suplantación de KDC) durante la autenticación de registro, la autenticación de Kerberos que utiliza rangos en minúsculas siempre falla.
- Kerberos V5 para PPP PAP y CHAP puede bloquear el router. Esto se corrigió en la versión 11.2(6) del software del IOS de Cisco.Consulte Cisco bug ID CSCdj08828 (sólo clientes registrados) .La solución temporal para esto es forzar el inicio de sesión exec en el router a través del **modo asíncrono interactivo** sin **autoselect durante el login** y luego hacer que el usuario inicie PPP manualmente:
  ```
  aaa authentication ppp default if-needed krb5 local
  ```
- Kerberos V5 no realiza la autorización ni la contabilización. Necesita otro código para hacerlo.

Configuración del router del IOS de Cisco

La configuración de esta sección representa un router AS5200 completamente configurado que ejecuta Kerberos V5. El router en esta configuración utiliza el servidor Kerberos para autenticar tanto las sesiones VTY como los usuarios que marcan para hacer PPP con la autenticación PAP.

Configuración 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
```

Configuración de Kerberos KDC

Asegúrese de tener los puertos adecuados configurados para **inetd**.

Nota: En este ejemplo se utilizan envolturas. Si desea encriptar Telnet, debe reemplazar Telnet normal por Telnet con kerberized, de modo que estos archivos tengan una apariencia diferente.

Configuración de puertos para 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
-----------------------------------------------------------------
```

Configuración de Archivos de Configuración Kerberos

A continuación, debe configurar algunos archivos de configuración Kerberos que lea el servidor KDC. Para obtener más información sobre el significado de estos parámetros, refiérase a la Guía de Instalación de Kerberos o a la Guía de Administración del Sistema.

```
# 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
     }
```

Configuración de la Base de Datos para el Servidor KDC

A continuación, debe crear la base de datos que utiliza el servidor de KDC.

1. Ingrese el 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:
```

Esto es necesario para recuperar la contraseña **srvtab** del router a través de TFTP con el comando **kerberos srvtab remote**.

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

2. Para agregar directores y usuarios a la base de datos, utilice el 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. Agregar un usuario:

```
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. Obtener una lista de la base de datos actual:

```
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. Agregue la entrada para el 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. Extraiga una clave de la tabla para el 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. Eche otro vistazo a la base de datos:

```
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. Mueva el archivo keytab a un lugar donde el router pueda llegar a él:

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

9. Inicie el servidor KDC:

```
# kdc/krb5kdc
#
```

10. Verifique para asegurarse de que se ejecute realmente:

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

11. Obligar al router a leer su entrada de tabla de claves:

```
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. Verifique el router para asegurarse de que todo está listo:

```
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. Active la depuración e intente iniciar sesión en el 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
```

Ejemplo de resultado del comando debug

Este es un usuario PPP que se autentica correctamente.

```
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
```

Troubleshoot

Esta sección contiene varios escenarios de posibles problemas. Estas depuraciones le ayudan a ver rápidamente un problema.

Nombre de rango incorrecto

```
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 no funciona

```
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
                                        ~~~~
```

El reloj del router no es correcto

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

Esto es lo que ve el usuario:

```
$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:
```

Cliente No En Base De Datos 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
```

El cliente está en la base de datos pero utiliza una contraseña incorrecta

```
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
```

El usuario ve este resultado:

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


User Access Verification

Username: cisco1
Password:
% Access denied

Username:
```

Entrada SRVTAB no correcta en el 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
```

Esto es lo que ve el usuario:

```
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:
```

Referencias

1. *Guía* del *administrador del sistema* Kerberos V5 (se incluye en un archivo comprimido y comprimido)
2. *Guía de instalación* Kerberos V5
3. *Guía del usuario* Kerberos V5 *UNIX*
4. Kerberos: Network Authentication Protocol
5. Servicio de autenticación de red Kerberos (USC/ISI's GOST Group)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. "Kerberos: Un servicio de autenticación para sistemas de red abierta ", USENIX Mar 1988
7. S P. Miller, B. C. Neuman, J. Yo. Schiller y J. H. Saltzer, "Kerberos Authentication and Authorization System", 21/12/87
8. R. M. Needham y M. D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers", Comunicaciones de ACM, Vol. 21(12), pp. 993-999 (diciembre de 1978)
9. V. L. Voydock y S. T. Kent, "Security Mecms in High-Level Network Protocols", *Computing Surveys*, vol. 15(2), ACM (junio de 1983)
10. Li Gong, "A Security Risk of Depender on Synchronized Clocks", *Operating Systems Review*, Vol 26, #1, pp 49-53
11. C. Neuman y J. Kohl, "The Kerberos Network Authentication Service (V5)", RFC 1510, septiembre de 1993
12. B Clifford Neuman y Theodore Ts'o, "Kerberos: Un servicio de autenticación para redes informáticas", IEEE Communications, 32(9), septiembre de 1994**Nota:** Muchos de estos documentos, que incluyen el de Neuman, Schiller y Steiner (#9) también están disponibles a través de FTP desde MIT Athena System — Kerberos Documentation . Para obtener copias de RFC, consulte Obtención de RFCs y Documentos de Estándares.

Información Relacionada

- Página de soporte de Kerberos
- Soporte Técnico - Cisco Systems