Resolviendo problemas y configurando el soporte de cliente del Kerberos V5

Contenido

Introducción

Este documento proporciona un ejemplo de configuración, así como algunas soluciones a los problemas comunes. Las técnicas que le ayudan a resolver problemas cualquier problema también se proporcionan en este documento. Este documento no dirige soporte de Telnet orientado a Kerberos.

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

Este documento asume que usted ha compilado y ha instalado correctamente una versión actual de la versión 5 del paquete del Kerberos del MIT. Refiera a las referencias en el extremo de este

artículo para información en cómo obtener, compilar, y instalar el Kerberos V5.

También observe que la versión 11.2 del Cisco IOS ® Software o más adelante está requerida para el soporte del Kerberos V5. Esto proporciona el soporte completo de la autenticación de cliente del Kerberos V, que incluye el reenvío de la credencial. Los sistemas que tienen infraestructuras del Kerberos V pueden utilizar sus centros de distribución de claves (KDC) para autenticar a los usuarios finales para la red o el acceso al router. Esto es una implementación del cliente y no una implementación del Kerberos KDC.

El Kerberos se considera un servicio de seguridad de la herencia y es el más beneficioso de las redes que utilizan ya el Kerberos.

Refiera a los Release Note del Cisco IOS Software Release 11.2 para más información detallada cuyo las versiones incluyen este soporte.

Para el soporte del Kerberos en las versiones de Cisco IOS Software subsiguientes, refiera al Software Advisor (clientes registrados solamente).

prerrequisitos

Requisitos

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.

- Cisco IOS Software Release 11.2 y Posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Introducción a Kerberos

El Kerberos es un Network Authentication Protocol para el uso en físicamente las redes inseguras. El Kerberos se basa en el modelo de la distribución de claves presentado por Needham y el Schroeder. (Véase el número 9 en la sección de referencias de este documento. Es diseñado para proporcionar la autenticación robusta para el cliente/las aplicaciones del servidor por el uso de la criptografía de clave secreta. Permite las entidades que comunican sobre las redes para probar su identidad el uno al otro mientras que evita el escuchar detras de las puertas o los ataques con paquetes copiados. También prevé la integridad de la secuencia de datos (tal

como detección de modificación) y el secreto (tal como prevención de la lectura no autorizada) con la ayuda de los sistemas de criptografía tales como DES.

Muchos de los protocolos usados en Internet no proporcionan ninguna Seguridad. Las herramientas usadas “para oler” las contraseñas apagado de la red están de uso corriente por los intrusos de sistemas. Así, las aplicaciones que envían una contraseña sobre la red no encriptada son vulnerables. También, otro cliente/aplicaciones del servidor confía en el programa del cliente para ser “honestos” sobre la identidad del usuario que la utiliza. Otras aplicaciones confían en el cliente para restringir sus actividades a las que se permita hacer, sin la otra aplicación por el servidor.

Algunos sitios intentan utilizar los Firewall para solucionar sus problemas de seguridad de red. Los Firewall asumen que “los malos” están en el exterior, que es a menudo una suposición inválida. Sin embargo, a los iniciados ha realizado a la mayoría de los incidentes del crimen informático que causan más daño. Los Firewall también tienen una desventaja significativa en que restringen cómo sus usuarios pueden utilizar Internet.

El Kerberos fue creado por el MIT como solución a estos problemas de seguridad de red. El protocolo Kerberos utiliza la criptografía profunda, de modo que un cliente pueda probar su identidad a un servidor (y vice versa) a través de una conexión de red insegura. Después de que un cliente y servidor haya utilizado el Kerberos para probar su identidad, él puede también cifrar todas sus comunicaciones para asegurar la aislamiento y la integridad de los datos mientras que él va alrededor su negocio.

El Kerberos es libremente disponible desde MIT, bajo un aviso del permiso de los derechos reservados que sea similar al que está usado para el funcionamiento BSD y el sistema de Windowing (Ventanas) X11. El MIT proporciona el Kerberos en la forma de origen. Se hace esto de modo que cualquier persona que desea utilizarlo pueda mirar sobre el código para ellos mismos y asegurarse que el código es digno de confianza. Además, para los que prefieran confiar en profesionalmente un producto admitido, el Kerberos está disponible como producto de muchos diversos vendedores.

El soporte de cliente del Kerberos V5 se basa en el sistema de autenticación de Kerberos desarrollado en el MIT. Bajo el Kerberos, un cliente (generalmente un usuario o un servicio) envía un pedido un boleto al Key Distribution Center (KDC). El KDC crea un servicio de concesión de vales (TGT) para el cliente, lo cifra con la ayuda de la contraseña del cliente como la clave, y envía el TGT cifrado de nuevo al cliente. El cliente entonces intenta desencriptar el TGT, con la ayuda de su contraseña. Si el cliente desencripta con éxito el TGT por ejemplo, si el cliente da la contraseña correcta), guarda el TGT desencriptado. Esto indica la prueba de la identidad del cliente.

El TGT, que expira en un tiempo especificado, permite que el cliente obtenga los boletos adicionales, que dan el permiso para los servicios específicos. Las peticiones y las concesiones de estos boletos adicionales son usuario-transparentes.

Puesto que el Kerberos negocia autenticado, se cifra opcionalmente, y comunica entre cualquier dos puntas en Internet, él proporciona una capa de Seguridad que no sea dependiente sobre qué lado de un Firewall localizan cualquier cliente. El Kerberos se utiliza sobre todo en los protocolos de nivel de aplicación (nivel del modelo ISO 7), tal como Telnet o FTP, para proporcionar al usuario para recibir la Seguridad. También se utiliza, aunque menos con frecuencia, como el sistema de autenticación implícito de secuencia de datos (tal como SOCK_STREAM) o de mecanismos RPC (nivel modelo ISO 6). Puede también ser utilizado en un nivel inferior para la Seguridad del host-a-host, en los protocolos tales como IP, UDP, o TCP (niveles modelo ISO 3 y

4). Aunque, tales implementaciones sean raras, si existen en absoluto.

Preve la autenticación recíproca y la comunicación segura entre los principales en una red abierta por la fabricación de claves secretas para cualquier solicitante. Un mecanismo para que estas claves secretas sean propagadas con seguridad a través de la red también se proporciona. El Kerberos no prevé la autorización o las estadísticas. Sin embargo, aplicaciones que desean al uso de la poder sus claves secretas para realizar esas funciones con seguridad.

Definiciones

- **Autenticación** — Asegúrese de que usted sea quién usted le dice es, y de que conocemos quién usted es.
- **Cliente** — Una entidad que puede obtener un boleto. Esta entidad es generalmente usuario o un host.
- **Credenciales** — Lo mismo que los boletos.
- **Daemon** — Un programa, generalmente uno que se ejecute en un host UNIX, ese mantiene los pedidos de red para la autenticación.
- Ordenador del **Host-a** que se puede acceder sobre una red.
- **Caso** — La segunda parte de un mandante identidad única de Kerberos. Da la información que califica el primario. El caso puede ser nulo. En el caso de un usuario, el caso es de uso frecuente para describir el uso previsto de las credenciales correspondientes. En el caso de un host, el caso es el nombre de host calificado completamente.
- **Kerberos** — En mitología griega, el perro tres-dirigido que guarda la entrada al mundo terrenal. En el mundo de la informática, el Kerberos es un paquete de la seguridad de la red que fue desarrollado en el MIT.
- **KDC** — Key Distribution Center. Una máquina esa boletos del Kerberos de los problemas.
- **Keytab** — Un archivo de tabla dominante que contiene una o más claves. Un host o un servicio utiliza un archivo keytab de la misma forma que un usuario utiliza su contraseña.
- **NAS** — Un servidor de acceso a la red (un cuadro de Cisco) o cualquier otra cosa que hacen autenticación de TACACS+ y los pedidos de autorización, o envía los paquetes de las estadísticas.
- **Principal** — Una cadena que nombra una entidad específica a la cual un conjunto de las credenciales pueda ser asignado. Tiene generalmente tres porciones nombradas Primary, caso, y REINO.El formato típico de un principal típico Kerberos es **primario/instanceREALM**.
- **Primario** — La primera parte de un mandante identidad única de Kerberos. En el caso de un usuario, es el nombre de usuario. En el caso de un servicio, es el nombre del servicio.
- **REINO** — La red lógica sirvió por una sola base de datos Kerberos y un conjunto de los centros de distribución de claves. Por el convenio, los Nombres de terreno son generalmente todas las letras mayúsculas, distinguir el reino del dominio de Internet.
- **Servicio** — Cualquier programa u ordenador que usted acceda sobre una red. Los ejemplos de los servicios incluyen:“host” — un host, (por ejemplo, cuando usted utiliza Telnet y el rsh)“ftp” — FTPautenticación del “krbtgt” —; por ejemplo el ticket distribuido“estallido” — Email
- **Boleto** — Un establecimiento temporario de credenciales electrónicas que verifica la identidad de un cliente para un servicio determinado.
- **TGT** — Ticket distribuido. Un boleto especial del Kerberos que permite que el cliente obtenga el Kerberos adicional marca dentro del mismo terreno de Kerberos.Una buena analogía para el ticket distribuido es un paso de tres días del esquí que es bueno en cuatro diversos centros

turísticos. Usted muestra el paso en cualquier centro turístico usted decide ir (hasta que expira), y usted recibe un boleto de la elevación para ese centro turístico. Una vez que usted tiene el boleto de la elevación, usted puede esquiar todos lo que usted quiere en ese centro turístico. Si usted va a otro centro turístico el next day, usted muestra de nuevo su paso, y usted consigue un boleto adicional de la elevación para el nuevo centro turístico. La diferencia es que el Kerberos V5 programa el aviso que usted tiene el paso del esquí del fin de semana, y consigue el boleto de la elevación para usted, así que usted no tenga que realizar las transacciones usted mismo.

Gotcha

Esta sección enumera varios elementos de los cuales usted necesite ser consciente:

- Aseegurese le quitar todos los espacios finales en los archivos de configuración. Los espacios finales pueden causar los problemas con el servidor krb5kdc. Si no, usted puede conseguir un mensaje que diga, "krb5kdc no puede comenzar la base de datos para el reino."
- Aseegurese el reloj en el router se fija al mismo tiempo que el host UNIX que funciona con al servidor KDC. Para evitar que los intrusos reajusten sus relojes del sistema para continuar utilizando los boletos expirados, el Kerberos V5 se configura para rechazar las peticiones del boleto de cualquier host cuyo reloj no esté dentro de la desviación máxima del reloj especificada del KDC (como se especifica en el archivo kdc.conf). Semejantemente, configuran a los host para rechazar las respuestas de cualquier KDC cuyo reloj no esté dentro de la desviación máxima del reloj especificada del host (como se especifica en el archivo krb5.conf). El valor predeterminado para la desviación máxima del reloj es 300 segundos (cinco minutos).
- Aseegurese los trabajos DNS correctamente. Varios aspectos del Kerberos confían en el servicio de nombre. Para que el Kerberos proporcione su alto nivel de seguridad, es más sensible a los problemas del servicio de nombre que algunas otras partes de su red. Es importante que sus entradas del Domain Name System (DNS) y sus host tienen la información correcta. Cada canónico del nombre del host debe ser el nombre del host calificado completamente (que incluye el dominio), y cada dirección IP del host debe reverso-resolución al nombre canónico.
- El soporte del Kerberos V5 del Cisco IOS no permite el uso de los nombres de terreno en minúscula y el código del Kerberos en el Cisco IOS no autentica a los usuarios si el reino está en minúsculas. Esto fue reparada en el Cisco IOS Software Release 11.2(7).Refiera al Id. de bug Cisco CSCdj10598 (clientes registrados solamente).La única solución alternativa es utilizar los Nombres de terreno mayúsculos (que es convencional).Los de terrenos en minúscula trabajan para extraer un TGT, pero no los credenciales del servicio. Puesto que Cisco utiliza su nuevo TGT para extraer los credenciales del servicio (usados para prevenir el ataque de simulación KDC) durante la autenticación de registración, la autenticación de Kerberos que utiliza los de terrenos en minúscula falla siempre.
- El Kerberos V5 para PPP PAP y GRIETA puede causar un crash al router. Esto fue reparada en el Cisco IOS Software Release 11.2(6).Refiera al Id. de bug Cisco CSCdj08828 (clientes registrados solamente).La solución alternativa para esto es forzar exec login en el router vía el **modo asincrónico interactivo** sin el durante-**login del autoselect** y después tener el comienzo PPP del usuario manualmente:`aaa authentication ppp default if-needed krb5 local`
- El Kerberos V5 no hace la autorización o las estadísticas. Usted necesita un cierto otro

código para hacer esto.

Configuración del router de Cisco IOS

La configuración en esta sección representa a un router de configuración completa AS5200 que haga el Kerberos V5. El router en esta configuración utiliza al servidor de Kerberos para autenticar las sesiones VTY y a los usuarios que dial adentro para hacer el PPP con la autenticación PAP.

Config AS5200 con el 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

Aseegurese le tener los puertos apropiados configurados para el **inetd**.

Nota: Este ejemplo utiliza los wrappers. Si usted quiere Telnet cifrado, usted necesita substituir la telnet normal por el Telnet kerberizado, así que estos archivos tienen un diverso aspecto.

Puertos de la configuración para el 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
-----------------------------------------------------------------
```

Archivos de configuración del Kerberos de la configuración

Después, usted necesita configurar algunos archivos de configuración del Kerberos que el servidor KDC lea. Para más información sobre lo que significan estos parámetros, refiera al Kerberos instalan la guía o la guía del System Admin .

```
# 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
     }
```

Configure la base de datos para el servidor KDC

Después, usted necesita crear la base de datos que el servidor KDC utiliza.

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 extraer la **contraseña srvtab del** router vía el TFTP con el **comando kerberos srvtab remote**.# **kadmin/dbutil/kdb5_util stash -r CISCO.EDU** Enter KDC database master key:

2. Para agregar los directors y a los 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. Agregue a 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. Consiga 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 a 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. Tome otra mirada en 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 está capaz el router de conseguirle:# cp /etc/krb5.keytab /ts/
   # chmod 777 /ts/krb5.keytab
9. Encienda al servidor KDC:# kdc/krb5kdc
   #
10. Marque para aseegurarse lo se ejecuta realmente:# ps -A | grep 'krb5'
    6043 ?? I 0:00.01 kdc/krb5kdc
    23427 ttypf S + 0:00.05 grep krb5
11. Fuerce al router a leer su entrada de tabla dominante: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. Marque al router para aseegurarse 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. Dé vuelta encendido a hacer el debug de e intente registrar 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

Aquí está un usuario PPP que autentica con éxito.

`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`

Troubleshooting

Esta sección contiene los diversos escenarios por problemas potenciales. Estos debugs le ayudan a ver rápidamente un problema.

Nombre de terreno 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
```

El DNS no trabaja

```
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
                                          ~~~~
```

Reloj del router no 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
----------------------
```

Aquí 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 la 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 las aplicaciones perjudican la contraseña

```
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 esta salida:

```
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
```

Aquí 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. *La guía de administrador de sistema del* Kerberos V5 (viene en un archivo cubierto de alquitrán, g-comprimido)
2. *Guía de instalación del* Kerberos V5
3. *La guía de usuario de Unix del* Kerberos V5
4. Kerberos: El Network Authentication Protocol
5. Servicio de autenticación de red Kerberos (grupo del GOST USC/ISI)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. "Kerberos: Un servicio de autenticación para los sistemas de red abierta ", USENIX marzo de 1988
7. S. P. Miller, A.C. Neuman, J.I. Schiller, y J.H. Saltzer, "autenticación de Kerberos y sistema de autorización,", 12/21/87
8. R. M. Needham y M.D. Schroeder, "usando la encripción para autenticación en las Redes grandes de las Computadoras," comunicaciones del ACM, vol. 21(12), 993-999 págs. (diciembre de 1978)
9. V. L. Voydock y S.T. Kent, "mecanismos de seguridad en los protocolos de red de alto nivel," *Sondeos de computación*, vol. 15(2), ACM (junio de 1983)

10. Gongo de Li, “un riesgo de seguridad dependiendo de relojes sincronizados”, *estudio de sistemas operativos*, vol. 26, #1, pp 49-53
11. C. Neuman y J. Kohl, “servicio de autenticación de red Kerberos (RFC 1510 del V5),", septiembre de 1993
12. B. Clifford Neuman y Theodore Ts'o, “Kerberos: Un servicio de autenticación para las redes informáticas,” Comunicaciones IEEE, 32(9), septiembre de 1994**Nota:** Muchos de estos documentos, eso incluyen el que está por Neuman, Schiller, y Steiner (#9) está también disponible vía el FTP del sistema de Antena MIT -- Documentación de Kerberos . Para obtener las copias de los RFC, refiera a los RFC y a los documentos de obtención de los estándares.

Información Relacionada

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