Troubleshooting e Configuração do Suporte ao Cliente Kerberos V5

Contents

Introduction

Este documento fornece um exemplo de configuração, bem como algumas soluções para problemas comuns. As técnicas que o ajudam a solucionar qualquer problema também são fornecidas neste documento. Este documento não aborda o suporte Telnet kerberizado.

A maior parte desse material deste artigo veio da documentação disponível gratuitamente fornecida com Kerberos e de várias perguntas frequentes (FAQs) disponíveis no pacote. As configurações vieram de um roteador funcional e de um servidor KDC Kerberos.

Este documento pressupõe que você compilou e instalou corretamente uma versão atual da versão 5 do pacote Kerberos do MIT. Consulte as referências no final deste artigo para obter informações sobre como obter, compilar e instalar o Kerberos V5.

Observe também que o Cisco IOS® Software Release 11.2 ou posterior é necessário para suporte a Kerberos V5. Isso oferece suporte total à autenticação de cliente Kerberos V, que inclui o encaminhamento de credenciais. Os sistemas com infraestrutura Kerberos V podem usar seus KDCs (Key Distribution Centers, Centros de Distribuição de Chaves) para autenticar usuários finais para acesso à rede ou ao roteador. Esta é uma implementação de cliente e não uma implementação Kerberos KDC.

Kerberos é considerado um serviço de segurança legado e é mais benéfico em redes que já usam Kerberos.

Consulte as notas da versão 11.2 do software Cisco IOS para obter informações mais detalhadas sobre quais versões incluem esse suporte.

Para suporte a Kerberos nas versões subsequentes do Cisco IOS Software, consulte o Software Advisor (somente clientes registrados) .

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco IOS versão 11.2 e posterior

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.

Conventions

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

Introdução ao Kerberos

Kerberos é um protocolo de autenticação de rede para uso em redes fisicamente inseguras. Kerberos é baseado no modelo de distribuição principal apresentado por Needham e Schroeder. (Consulte o Número 9 na seção Referências deste documento. Ele foi projetado para fornecer autenticação forte para aplicativos cliente/servidor com o uso de criptografia de chave secreta. Ele permite que as entidades que se comunicam através de redes provem sua identidade entre si enquanto evita escutas ou ataques repetidos. Ele também fornece integridade de fluxo de dados (como detecção de modificação) e sigilo (como prevenção de leitura não autorizada) com a ajuda de sistemas de criptografia como DES.

Muitos dos protocolos usados na Internet não fornecem nenhuma segurança. As ferramentas usadas para "farejar" senhas da rede estão em uso comum por invasores de sistemas. Assim, os aplicativos que enviam uma senha pela rede não criptografada são vulneráveis. Além disso,

outros aplicativos cliente/servidor dependem do programa cliente para serem "honestos" sobre a identidade do usuário que o usa. Outros aplicativos dependem do cliente para restringir suas atividades àquelas que ele tem permissão para fazer, sem nenhuma outra aplicação por parte do servidor.

Alguns sites tentam usar firewalls para resolver seus problemas de segurança de rede. Os firewalls presumem que "os bandidos" estão por fora, o que muitas vezes é uma suposição inválida. No entanto, a maioria dos incidentes de crimes de computador que causam mais danos foram realizados por pessoas de dentro. Os firewalls também têm uma desvantagem significativa, pois restringem a forma como os usuários podem usar a Internet.

Kerberos foi criado pelo MIT como uma solução para esses problemas de segurança de rede. O protocolo Kerberos usa criptografia forte, de modo que um cliente possa provar sua identidade para um servidor (e vice-versa) através de uma conexão de rede insegura. Depois que um cliente e um servidor usam Kerberos para provar sua identidade, eles também podem criptografar todas as suas comunicações para garantir a privacidade e a integridade dos dados enquanto fazem negócios.

Kerberos está disponível gratuitamente no MIT, sob um aviso de permissão de copyright semelhante ao usado para o sistema operacional BSD e o sistema de janelamento X11. O MIT fornece Kerberos na forma de origem. Isso é feito para que qualquer pessoa que deseje usá-lo possa olhar o código para si e assegurar-se de que o código é confiável. Além disso, para quem prefere confiar em um produto com suporte profissional, o Kerberos está disponível como um produto de vários fornecedores diferentes.

O suporte ao cliente Kerberos V5 é baseado no sistema de autenticação Kerberos desenvolvido no MIT. Em Kerberos, um cliente (geralmente um usuário ou um serviço) envia uma solicitação de um tíquete para o Centro de Distribuição de Chaves (KDC). O KDC cria um tíquete de concessão de tíquete (TGT) para o cliente, criptografa-o com a ajuda da senha do cliente como a chave e envia o TGT criptografado de volta ao cliente. Em seguida, o cliente tenta descriptografar o TGT, com a ajuda de sua senha. Se o cliente descriptografar com êxito o TGT, por exemplo, se o cliente fornecer a senha correta), ele manterá o TGT descriptografado. Isso indica a prova da identidade do cliente.

A TGT, que expira em um horário especificado, permite que o cliente obtenha tíquetes adicionais, que dão permissão para serviços específicos. As solicitações e concessões desses tíquetes adicionais são transparentes para o usuário.

Como o Kerberos negocia autenticado, é opcionalmente criptografado e se comunica entre dois pontos na Internet, ele fornece uma camada de segurança que não depende de qual lado do firewall um cliente está localizado. Kerberos é usado principalmente em protocolos de nível de aplicação (modelo ISO nível 7), como Telnet ou FTP, para fornecer segurança de usuário para host. Ele também é usado, embora com menos frequência, como o sistema de autenticação implícita do fluxo de dados (como SOCK_STREAM) ou mecanismos RPC (modelo ISO nível 6). Ele também pode ser usado em um nível mais baixo para segurança host a host, em protocolos como IP, UDP ou TCP (modelos ISO Níveis 3 e 4). Embora tais implementações sejam raras, se é que existem.

Ele fornece autenticação mútua e comunicação segura entre os principais em uma rede aberta pelo fabrico de chaves secretas para qualquer solicitante. Também é fornecido um mecanismo para que essas chaves secretas sejam propagadas com segurança através da rede. O Kerberos não fornece autorização ou contabilidade. No entanto, os aplicativos que desejam podem usar suas chaves secretas para executar essas funções com segurança.

Definições

- **Autenticação** — Certifique-se de que você é quem diz ser e de que sabemos quem você é.
- **Cliente** — Uma entidade que pode obter um tíquete. Essa entidade é geralmente um usuário ou um host.
- **Credenciais** — O mesmo que tíquetes.
- **Daemon** — Um programa, geralmente executado em um host UNIX, que atende às solicitações de autenticação de rede.
- **Host** —Um computador que pode ser acessado através de uma rede.
- **Instância** — A segunda parte de um principal Kerberos. Ele fornece informações que qualificam o principal. A instância pode ser nula. No caso de um usuário, a instância é frequentemente usada para descrever o uso pretendido das credenciais correspondentes. No caso de um host, a instância é o nome de host totalmente qualificado.
- **Kerberos** — Na mitologia grega, o cachorro de três cabeças que guarda a entrada do submundo. No mundo dos computadores, Kerberos é um pacote de segurança de rede que foi desenvolvido no MIT.
- **KDC** — Centro de Distribuição de Chaves. Uma máquina que emite tíquetes Kerberos.
- **Keytab** — Um arquivo-chave da tabela que contém uma ou mais teclas. Um host ou serviço usa um arquivo de guia de chave da mesma forma que um usuário usa sua senha.
- **NAS** — Um servidor de acesso à rede (uma caixa da Cisco) ou qualquer outra coisa que faça solicitações de autenticação e autorização TACACS+ ou envie pacotes de contabilidade.
- **Principal** — Uma string que nomeia uma entidade específica à qual um conjunto de credenciais pode ser atribuído. Ele geralmente tem três partes chamadas Primário, Instância e REALM.O formato típico de um principal Kerberos típico é **primary/instanceREALM**.
- **Primário** — A primeira parte de um principal Kerberos. No caso de um usuário, é o nome de usuário. No caso de um serviço, é o nome do serviço.
- **REALM** —A rede lógica servida por um único banco de dados Kerberos e um conjunto de Centros de Distribuição Principais. Por convenção, os nomes de território são geralmente letras maiúsculas, para diferenciar o domínio do domínio da Internet.
- **Serviço**: qualquer programa ou computador que você acessa em uma rede. Exemplos de serviços incluem:"host"—um host (por exemplo, quando você usa Telnet e rsh)"ftp"—FTP"krbtgt"—autenticação; como a emissão de um bilhete"pop"—E-mail
- **Tíquete** —Um conjunto temporário de credenciais eletrônicas que verifica a identidade de um cliente para um serviço específico.
- **TGT** — Bilhete de Concessão de Bilhetes. Um tíquete Kerberos especial que permite que o cliente obtenha tíquetes Kerberos adicionais no mesmo território Kerberos.Uma boa analogia para o bilhete é um passe de esqui de três dias que é bom em quatro diferentes resorts. Você mostra o passe em qualquer resort em que decidir ir (até que ele expire) e recebe um tíquete de elevação para esse resort. Uma vez que você tenha o bilhete de elevador, você pode esquiar tudo o que quiser naquele resort. Se você for para outro recurso no dia seguinte, mostre novamente seu passe e obterá um tíquete de elevação adicional para o novo resort. A diferença é que os programas Kerberos V5 notam que você tem o passe de esqui no fim de semana e recebe o bilhete de elevador para você, então você mesmo não precisa realizar as transações.

Te peguei

Esta seção lista vários itens dos quais você precisa estar ciente:

- Certifique-se de remover todos os espaços finais nos arquivos de configuração. Espaços de triagem podem causar problemas com o servidor krb5kdc. Caso contrário, você pode receber uma mensagem que diz, "o krb5kdc não pode iniciar o banco de dados para o território".
- Certifique-se de que o relógio no roteador esteja definido ao mesmo tempo que o host UNIX que executa o servidor KDC. Para impedir que os invasores redefinam seus relógios de sistema para continuar a usar tíquetes expirados, o Kerberos V5 é configurado para rejeitar solicitações de tíquete de qualquer host cujo relógio não esteja dentro do limite máximo de tempo especificado do KDC (conforme especificado no arquivo kdc.conf). Da mesma forma, os hosts são configurados para rejeitar respostas de qualquer KDC cujo relógio não esteja dentro do limite máximo de tempo especificado do host (conforme especificado no arquivo krb5.conf). O valor padrão para desvio máximo do relógio é 300 segundos (cinco minutos).
- Verifique se o DNS funciona corretamente. Vários aspectos do Kerberos dependem do serviço de nome. Para que o Kerberos forneça seu alto nível de segurança, ele é mais sensível a problemas de serviço de nomes do que outras partes da sua rede. É importante que as entradas do Sistema de Nomes de Domínio (DNS) e os hosts tenham as informações corretas. Cada canônico do nome de host deve ser o nome de host totalmente qualificado (que inclui o domínio), e cada endereço IP do host deve ser solucionado de forma inversa para o nome canônico.
- O suporte a Kerberos V5 do Cisco IOS não permite o uso de nomes de territórios minúsculos e o código Kerberos no Cisco IOS não autentica usuários se o território estiver em minúsculas. Isso foi corrigido no Cisco IOS Software Release 11.2(7).Consulte o bug da Cisco ID CSCdj10598 (somente clientes registrados) .A única solução alternativa é usar nomes REALM maiúsculos (o que é convencional).Os territórios em minúsculas funcionam para recuperar uma TGT, mas não uma credencial de serviço. Como a Cisco usa seu novo TGT para recuperar uma credencial de serviço (usada para evitar o ataque de falsificação KDC) durante a autenticação de registro, a autenticação Kerberos que usa territórios minúsculos sempre falha.
- Kerberos V5 para PPP PAP e CHAP podem travar o roteador. Isso foi corrigido no Cisco IOS Software Release 11.2(6).Consulte o bug da Cisco ID CSCdj08828 (somente clientes registrados) .A solução alternativa para isso é forçar o login exec no roteador via **modo assíncrono interativo** sem **autoseleção durante o login** e, em seguida, fazer com que o usuário inicie o PPP manualmente:
  ```
  aaa authentication ppp default if-needed krb5 local
  ```
- Kerberos V5 não faz autorização ou contabilidade. Você precisa de outro código para fazer isso.

Configuração do roteador do Cisco IOS

A configuração nesta seção representa um roteador AS5200 totalmente configurado que faz Kerberos V5. O roteador nesta configuração usa o servidor Kerberos para autenticar sessões VTY e usuários que discam para fazer PPP com autenticação PAP.

Config. AS5200 com 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
```

Configuração do KDC Kerberos

Verifique se você tem as portas corretas configuradas para **inetd**.

Observação: este exemplo usa wrappers. Se você deseja um Telnet criptografado, é necessário substituir o Telnet normal pelo Telnet com kerberized, de modo que esses arquivos tenham uma aparência diferente.

Configurar portas 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
-----------------------------------------------------------------
```

Configurar arquivos de configuração do Kerberos

Em seguida, você precisa configurar alguns arquivos de configuração Kerberos que o servidor KDC lê. Para obter mais informações sobre o que esses parâmetros significam, consulte o Guia de instalação do Kerberos ou o Guia de administração do 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
     }
```

Configurar o banco de dados para o servidor KDC

Em seguida, você precisa criar o banco de dados que o servidor KDC usa.

1. Digite o 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:
```

Isso é necessário para recuperar a senha **srvtab** do roteador via TFTP com o comando **kerberos srvtab remote**.

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

2. Para adicionar principais e usuários ao banco de dados, use o 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. Adicionar um usuário:

```
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. Obter uma lista do banco de dados atual:

```
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. Adicione a entrada para o roteador 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. Extraia uma chave para a tabela do roteador 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. Dê mais uma olhada no banco de dados:

```
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. Mova o arquivo keytab para um local onde o roteador possa chegar até ele:

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

9. Inicie o servidor KDC:

```
# kdc/krb5kdc
#
```

10. Verifique se ele realmente está em execução:

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

11. Forçar o roteador a ler sua entrada de tabela chave:

```
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 o roteador para ter certeza de que tudo está 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. Ative a depuração e tente fazer login no roteador:

```
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
```

Exemplo de saída de depuração

Aqui está um usuário PPP que autentica com êxito.

```
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 seção contém vários cenários para possíveis problemas. Essas depurações ajudam você a ver rapidamente um problema.

Nome do território errado

```
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
```

O DNS não 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
                                          ~~~~
```

Relógio do Roteador Não Correto

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

Aqui está o que o usuário vê:

```
$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 Não Está No Banco De Dados 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
```

O cliente está no banco de dados, mas usa a senha incorreta

```
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
```

O usuário vê esta saída:

```
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 não correta no roteador

```
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
```

Aqui está o que o usuário vê:

```
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:
```

Referências

1. *Guia do administrador do sistema* Kerberos V5 (vem em um arquivo gravado, g-zipado)
2. *Guia de instalação* do Kerberos V5
3. *Guia do usuário do UNIX* Kerberos V5
4. Kerberos: O Network Authentication Protocol
5. O Serviço de Autenticação de Rede Kerberos (Grupo GOST do USC/ISI)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. "Kerberos: An Authentication Service for Open Network Systems ", USENIX março de 1988
7. S. P. Miller, B. C. Neuman, J. Eu. Schiller e J. H. Saltzer, "Kerberos Authentication and Authorization System" (Sistema de autenticação e autorização Kerberos), 21/12/87
8. R. M. Needham e M. D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Communications of the ACM, vol. 21(12), pp. 993-999 (dezembro de 1978)
9. V. L. Voydock e S. T. Kent, "Security Mechanisms in High-Level Network Protocols", *Computing Surveys*, vol. 15(2), ACM (junho de 1983)
10. Li Gong, "A Security Risk of Dependendo dos Relógios Sincronizados", *Operating Systems Review*, Vol 26, #1, pp 49-53
11. C. Neuman e J. Kohl, "The Kerberos Network Authentication Service (V5)", RFC 1510, setembro de 1993
12. B. Clifford Neuman e Theodore Ts'o, "Kerberos: An Authentication Service for Computer Networks," IEEE Communications, 32(9), setembro de 1994**Observação:** muitos desses documentos, incluindo o de Neuman, Schiller e Steiner (#9) também estão disponíveis via FTP no MIT Athena System — Documentação Kerberos. Para obter cópias de RFCs, consulte Obtendo RFCs e Documentos de Padrões.

Informações Relacionadas

- Página de suporte do Kerberos
- Suporte Técnico - Cisco Systems